TESIS DE LA UNIVERSIDAD DE ZARAGOZA

2013

42

Guillermo I. Azuara Guillén

Desarrollo de un sistema exportable de confianza corporativa: aplicación a entornos de trazabilidad de productos

Departamento
Ingeniería Electrónica y Comunicaciones

Director/es
Salazar Riaño, José Luis

ISSN 2254-7606

Prensas de la Universidad Universidad Zaragoza

Universidad Zaragoza
1542

Tesis Doctoral

DESARROLLO DE UN SISTEMA EXPORTABLE DE CONFIANZA CORPORATIVA: APLICACIÓN A ENTORNOS DE TRAZABILIDAD DE PRODUCTOS

Autor

Guillermo I. Azuara Guillén

Director/es

Salazar Riaño, José Luis

UNIVERSIDAD DE ZARAGOZA

Ingeniería Electrónica y Comunicaciones

Departamento de
Ingeniería Electrónica
y Comunicaciones
Universidad Zaragoza

Instituto Universitario de Investigación
de Ingeniería de Aragón
Universidad Zaragoza

Tesis Doctoral

Universidad Zaragoza

Desarrollo de un sistema exportable de confianza corporativa. Aplicación a entornos de trazabilidad de productos.

Autor
Guillermo Azuara Guillén

Director
José Luis Salazar Riaño

Agradecimientos

Cuando se acerca el final del camino y miro hacia atrás, puedo ver las caras sonrientes de todos los que me han ayudado durante el trayecto. En las pendientes cortas pero escarpadas, en los llanos que se hacían interminables cuando no se divisaba la meta, y en las cuestas abajo, donde hacía falta la mente fría para no correr demasiado y caer.

Como dijo Virgilio: "Un camino sin obstáculos probablemente conduce a algún lugar que no vale la pena". Así que, aunque en el camino hubo tropiezos, siempre una mano amiga me ayudó a levantarme. Cuando me perdí, siempre encontré algún caminante que me indicó la dirección correcta. Cuando estaba cansado no me faltaron las palabras de aliento para continuar. Y muchas han sido las personas que han conseguido que el trayecto sea más llevadero.

Muchas gracias a todos los que han hecho posible el desarrollo de esta tesis. Gracias a mis padres, que con su esfuerzo y ejemplo siempre me han animado a seguir adelante.

Un agradecimiento especial a mis compañeros del Grupo de Tecnologías de las Comunicaciones en Teruel: Ana, Pedro y Ana, y también a Raúl y Eduardo. Gracias también a mis compañeros del área de Ingeniería Telemática en la Escuela de Ingeniería y Arquitectura, que han hecho que en mis visitas a Zaragoza me sintiera como en casa.

Gracias a José Luis mi director de tesis y a José Luis del observatorio de identidad digital de la cátedra telefónica de la Universidad de Zaragoza.

Tampoco quisiera olvidarme de las administraciones e instituciones que han colaborado en la financiación de las investigaciones que se han abordado en esta tesis: Instituto Nacional de Alimentación y Tecnología Agraria y Agroalimentaria, Cátedra Telefónica de la Universidad de Zaragoza, Comisión Interministerial de Ciencia y Tecnología, Ministerio de Educación y Ciencia, Ministerio de Ciencia e Innovación, Fondos Europeos de Desarrollo Regional y la Fundación Universitaria Antonio Gargallo.

Y para finalizar, y no menos importante, quería darle las gracias a Mamen por haber estado ahí todos estos años y a Rocío, que a pesar de sus cuatro años, es capaz de recargar la energía en los momentos más aciagos con sólo una sonrisa.

Seguro que me dejo a alguien, lamento el olvido, pero gracias de corazón.

"Cuando se viaja en pos de un objetivo, es muy importante prestar atención al Camino. El Camino es el que nos enseña la mejor forma de llegar y nos enriquece mientras lo estamos cruzando" (Paulo Coelho).

Resumen

Cada vez es más habitual que en los procesos de fabricación participen diversos fabricantes y empresas. Por otro lado, una característica de los productos muy valorada hoy en día por los consumidores, es la calidad. Ya no es suficiente con producir barato, sino que cada vez es más importante producir con calidad, siendo ésta un factor diferenciador de las manufacturas que se realizan bajo las diversas marcas.

La calidad se está integrando cada vez más en las empresas y en sus procesos productivos y de gestión, como un valor añadido y diferenciador del producto. Es habitual encontrar diversos controles de calidad a lo largo de los procesos de fabricación. Lo que ya no es tan habitual es que se pueda identificar a los operarios encargados del control de calidad. A lo sumo, el encargado del control de calidad final deja algún tipo de identificación (por ejemplo un pequeño adhesivo o etiqueta con un número impreso), pero esta identificación carece de sentido en cuanto el producto entra en otra cadena de producción o llega al comprador.

En este escenario, aparece otro factor importante como es la confianza. En los actuales sistemas productivos se deben establecer relaciones de confianza entre las empresas encargadas de las diferentes fases de producción (todas esperan que las demás hagan su trabajo según lo acordado). Además, los agentes designados para verificar la adecuación de los productos a lo esperado en las diversas fases de producción, son depositarios de la confianza de la empresa a la que pertenecen.

El objetivo principal de la tesis es el desarrollo de un modelo de confianza corporativa exportable, que sea sencillo y económico de implementar. Para ello, se ha propuesto un sistema confiable de identidad digital de los productos. Es decir, cada producto posee un conjunto de atributos que definen su identidad digital, que lo hace único, pero además, cada uno de estos atributos está avalado por el agente de control que lo verificó, por tanto se puede afirmar que es una identidad de calidad. Con este planteamiento, y con una infraestructura mínima, se pueden integrar en el sistema todos los procesos y compañías involucrados en la cadena de producción, bajo un sello de calidad común: la identidad de calidad del producto.

Para comprobar la validez de esta propuesta, se ha realizado una prueba de concepto, integrando este sistema de identidad de calidad en un entorno de trazabilidad alimentaria basada en RFID (identificación por radiofrecuencia).

Este prototipo, que sirve para securizar la trazabilidad de un producto cárnico elaborado, se ha realizado sobre la tecnología de etiquetado basada en RFID. Con esta tecnología, y para las condiciones ambientales donde se ha desarrollado el proceso de producción de las piezas a controlar en este caso concreto, el tipo de etiquetas idóneo dispone de una cantidad de memoria extremadamente reducida. Además, debido a que anualmente deben utilizarse unas 800.000 etiquetas, el coste de estas etiquetas debe ser sumamente bajo, por lo que sólo es posible utilizar etiquetas muy sencillas (y por tanto muy económicas).

Para poder utilizar este tipo de etiquetas, se ha planteado que las operaciones criptográficas no sean realizadas en la etiqueta, sino en un sistema externo basado en una Infraestructura de Clave Pública (*PKI*), de manera que la etiqueta sólo sirve como soporte de datos en texto plano (sin cifrar), pero firmados electrónicamente.

Para resolver el problema del poco espacio de memoria disponible para las firmas de los diferentes agentes de control, se ha recurrido a la utilización de firmas agregadas. Además, al trabajar con criptografía de curvas elípticas, el tamaño de la firma es notablemente menor, para un mismo nivel de seguridad, que el de otros sistemas.

Adicionalmente, el sistema propuesto permite transferir la confianza entre las compañías implicadas en un proceso de producción (basta compartir las claves públicas de los firmantes y sus nombres), y se adapta a cualquier entorno productivo.

Por todo ello, el sistema propuesto resuelve de forma eficaz la integración de diversas empresas en el proceso de fabricación de un producto, con escaso coste, y permitiendo una verificación de la identidad digital en cualquier parte del proceso, incluida la fase de comercialización.

Publicaciones

Revistas científicas internacionales

- **Guillermo Azuara**, José Luis Tornos, José Luis Salazar, "Improving RFID traceability systems with verifiable Quality", Industrial Management & Data Systems, Vol. 112 Iss: 3. 2012.

Congresos Internacionales

- **Azuara, G.**, Salazar, J.L., "Comprehensive protection of RFID traceability information systems using aggregate signatures", Lecture Notes in Computer Science, vol. 6694 LNCS, pp. 168-176, 2011.
- **G. Azuara**, J. L. Salazar, J. L. Tornos and J. J. Piles, "Reliable food traceability using RFID tagging," Lect. Notes Comput. Sci., vol. 6054 LNCS, pp. 57-67, 25 January 2010 through 28 January 2010, 2010.
- Piedad Garrido, Fernando Naranjo, Jesús Tramullas, Miguel Esteban, Ana López, **Guillermo Azuara**, Ana Salinas, Pedro Ramos, Eva Hervás and Eduardo Pascual, "Free traceability management using RFID and topic maps," in Proceedings of the 4th European Conference on Information Management and Evaluation, Lisbon, Portugal, 2010, pp. 93-103.
- A.M. López, E. Pascual, A.M. Salinas, P.Ramos y **G.Azuara**, "Design of a RFID Based Traceability System in a Slaughterhause", Workshops Proceedings of the 5th International Conference on Intelligent Environments, Volume 4 Ambient Intelligence and Smart Environments, ISBN: 978-1-60750-056-8. Octubre 2009.

Congresos nacionales

- Piedad Garrido, Fernando Naranjo, Ana López, **Guillermo Azuara** y Jesús Tramullas, "Uso de las tecnologías RFID y XTM para la trazabilidad en producción y logística de un matadero", Terceras Jornadas Científicas sobre RFID, Libro de actas, ISBN: 978-84-96997-27-1, pp. 197-201, Bilbao. Noviembre. 2009.
- **G. Azuara**, J.L. Salazar, "Protección integral de sistema de trazabilidad RFID mediante firmas agregadas", VIII Jornadas de Ingeniería Telemática, Libro de Actas, pp.: 197-201, ISBN: 978-84-96997-27-1. Septiembre. 2009.
- **G. Azuara**, J.J. Piles, J.L. Salazar, "Securización de un sistema de trazabilidad RFID mediante firmas agregadas", VII Jornadas de Ingeniería Telemática, Libro de Actas, pp.: 57-63. 2008.
- **G. Azuara Guillen**, J. L. Salazar Riaño. "Aplicación de firmas digitales agregadas a la trazabilidad de productos", XXIII Simposium Nacional de la Unión Científica Internacional de Radio (URSI 2008), Madrid, ISBN: Libro de actas, ISBN: 978-84-612-6291-5. Septiembre. 2008.

Proyectos de investigación e I+D directamente relacionados

- Título del proyecto: Sistema de Trazabilidad para el CRDO Jamón de Teruel. PET2007-08-C11-06.
  - Entidad financiadora: Instituto Nacional de Investigación y Tecnología Agraria y Agroalimentaria (INIA).
  - Entidades participantes: UNIVERSIDAD DE ZARAGOZA.
  - Duración, desde: 13-06-2007 hasta: 13-06-2009.

- Título del proyecto: Sistemas RFID de baja frecuencia. Estudio para su utilización en el sistema de trazabilidad de la Denominación de Origen Jamón de Teruel. 2008/B009
  - Entidad financiadora: Fundación Universitaria Antonio Gargallo
  - Entidades participantes: Universidad de Zaragoza
  - Duración, desde: 18-02-2008 hasta: 31-12-2008.

Índice general

Anexos

Índice de figuras

Índice de tablas

Acrónimos

3DES	*Triple Data Encryption Standard*
ABAC	*Attribute-Based Access Control*
AES	*Advanced Encryption Standard*
APPCC	*Análisis de Peligros y Puntos de Control Crítico*
CDH	*Computational Diffie-Hellman*
Co-DDH	*Decision co-Diffie-Hellman*
Co-GDH	*Co-Gap Diffie Hellman*
CRDO	*Consejo Regulador Denominación de Origen*
DDH	*Decision Diffie-Hellman*
DES	*Data Encryption Standard*
DoS	*Denial of Service*
DSA	*Digital Signature Algorithm*
ECC	*Elliptic Curve Cryptography*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
GDH	*Gap Diffie Hellman*
HF	*High Frequency*
IBC	*Identity-Based Cryptography*
IdM	*Identity Management*
IdP	*Identity Provider*
ISO	*International Organization for Standardization*
MD5	*Message Digest Algorithm 5*

MOV	*Menezes, Okamoto y Scott (tipo de ataque)*
NFC	*Near Field Communication*
NIST	*National Institute of Standards and Technology*
NO-SS	*No Supersingular*
PKG	*Private Key Generator*
PRNG	*Pseudorandom Number Generator*
QAS	*Quality Assurance System*
RBAC	*Role-Based Access Control*
REGA	*Registro General de Explotaciones Ganaderas*
RFID	*Radio Frequency Identification*
RSA	*Rivest, Shamir y Adelman (Sistema criptográfico)*
SHA	*Secure Hash Algorithm*
SP	*Service Provider*
SS	*Supersingular*
SSO	*Single Sing On*
UID	*Unique Identification Number*

1. Introducción

1.1. Motivación y objetivos

Un factor cada vez más valorado en los competitivos mercados globalizados es la calidad. Ya no sólo se compite en precio o plazo de entrega, sino que cada día es más necesario un nivel de calidad que permita a un producto o marca distinguirse de la competencia. El siguiente paso en este camino, es que esta calidad sea objetivamente medible e incluso lo ideal es que pueda ser verificada por todos los integrantes de la cadena de producción, incluido el usuario final como consumidor del producto.

Por este motivo, desde hace unos años se están implantando en muchos entornos de producción los sistemas de aseguramiento de la calidad (QAS, *Quality Assurance System*). Estos sistemas están diseñados para inspeccionar la calidad del producto, poder determinar las causas de las anomalías, analizar los datos de la cadena de producción y proponer un plan para solucionar los problemas. Las etapas de diseño e implementación de los QAS se pueden enumerar como: adquisición, análisis, acción y fase de auditoría [LYU2009].

Los sistemas QAS permiten mejorar la imagen de marca, diferenciándose de la competencia y aumentando la confianza del consumidor en el producto [KARLSEN2010]. Aunque hay sistemas de certificación voluntaria para mejorar la imagen de la empresa (como las certificaciones emitidas por terceras partes) [ALBERSMEIER2009], en algunos sectores el control de calidad y en especial la trazabilidad son obligatorios. Por ejemplo, en Europa, el uso de la trazabilidad alimentaria es un imperativo legal desde 2002 (Regulation (EC) Nº 178/2002).

Es también cada vez más habitual, que en el proceso de fabricación de un producto intervengan diferentes empresas, y por tanto es importante poder confiar en que cada una de ellas realiza su tarea de manera adecuada. Una manera de hacerlo, es verificar que tras cada fase de producción, los atributos del producto cumplen con los requisitos de calidad. Estos atributos, que en su conjunto conformarán la identidad digital del producto, junto con la firma digital del agente que los ha verificado, acompañarán al producto durante todo el proceso de fabricación y posterior comercialización.

Por otro lado, el uso de QAS supone la introducción en el sistema de marcas de certificación, auditorías externas o sistemas de trazabilidad [CARRIQUIRY2007]. Los sistemas de trazabilidad, añaden a las cadenas de producción y suministro "la posibilidad de identificar el origen y las diferentes etapas de un proceso de producción y distribución de bienes de

consumo"[1]. En este entorno, son muchos los estudios que presentan y cuantifican las ventajas de la trazabilidad de los productos [CHRYSSOCHOIDIS2009, HOBBS2004, MAI2010, XIAOJUN2006], por lo que parece interesante el desarrollar métodos que puedan garantizar la autenticidad de esa trazabilidad o de la calidad de los productos, dada las perspectivas de expansión y penetración en los sistemas productivos de estos elementos.

Hay diversos métodos de implementar la trazabilidad: códigos impresos en los productos, hojas de registro, sistemas electrónicos, etc… [MEHRJERDI2011]. La utilización de sistemas electrónicos de trazabilidad permiten superar los problemas inherentes a los sistemas manuales, como la eliminación de errores en la transcripción de datos, reducción en los tiempos y errores de inventario, reducción general de los tiempos de trabajo y en general un incremento de la velocidad de producción y una mayor eficiencia en el proceso [CHRYSSOCHOIDIS2009].

En esta tesis se desarrollará un sistema de confianza corporativa exportable, es decir un sistema que permita confiar en que un producto ha cumplido con todos los requisitos de calidad a lo largo de su proceso de fabricación, y que además sea aplicable a cualquier entorno de producción.

Este sistema de confianza se basa en una identidad digital confiable, y que como prueba de concepto, ha sido aplicado a la trazabilidad de productos cárnicos**.** Dicha identidad se conforma a través de rasgos identificativos adquiridos de forma supervisada, y ha sido desarrollada sobre sistemas basados en identificación electrónica, concretamente en el uso de identificación por radiofrecuencia (RFID). Como características concretas, se pueden indicar que los certificados digitales se expedirán ad-hoc, para avalar la autenticidad y el origen de una determinada información contenida en un soporte concreto, y que además serán fácilmente verificables por una tercera parte.

La integración del sistema de identidad digital con un sistema automatizado de captura de datos, añade un mayor nivel de protección a la cadena de suministro, haciéndolo más robusto frente a algunas de las amenazas inherentes a la tecnología RFID, sin olvidar que además de suministrar un sistema garante de la calidad, la trazabilidad ofrece "per sé"

[1] *Definición de "trazabilidad" dada por la Real Academia Española de la Lengua. En el apartado 2.2.1 se entrará más en detalle en la definición de trazabilidad.*

un sistema de protección contra las falsificaciones del producto. Este problema, las falsificaciones, supone un volumen económico cada vez más importante, con un crecimiento notable y que ya rebasaba los 200.000 millones de dólares anuales en el año 2007, sólo teniendo en cuenta la economía de Estados Unidos [MATOS2007]. De hecho, en los informes más recientes, como el elaborado por la consultora Frontier Economics [ECONOMICS2011], se prevé que para el año 2015 el volumen económico de falsificaciones y productos pirateados (software, audio y video) se mueva entre los 1.220.000 y 1.770.000 millones de dólares.

Así pues, el objetivo principal de esta tesis es proveer un sistema de identidad digital basada en atributos avalados por entidades confiables, que sea integrable en una cadena de producción.

Para que el sistema sea viable en productos que no tengan un valor añadido muy alto, es decir que no sean productos de lujo, es necesario que el precio de las etiquetas RFID sea muy reducido. Este condicionante hace que no puedan utilizarse la mayoría de los métodos que se basan en que las etiquetas realicen operaciones criptográficas, por lo que se optó por utilizar la etiqueta como mero soporte de toda la información en texto plano (sin cifrar), pero avalada por una firma digital que permite saber quién ha introducido los datos y que dichos datos no han sido modificados desde su firma.

Otro problema que hubo que resolver, también derivado del tipo de etiquetas a utilizar, fue la reducida cantidad de memoria disponible. Para optimizar el uso de este recurso, se recurrió al uso de firmas agregadas, de manera que todas las firmas que van acompañando a cada mensaje, se van compactando en una única firma de tamaño constante.

Por otro lado, teniendo en cuenta que las cadenas de producción pueden estar integradas por diversas empresas, el sistema también deberá contemplar este aspecto. Deberá permitirse que de una manera sencilla, los agentes de control de las diversas empresas implicadas, puedan introducir en la identidad digital del producto los atributos correspondientes, así como proceder a su firma.

Los agentes de control mencionados en el párrafo anterior, son depositarios de la confianza de la empresa a la que pertenecen. Por ello, también se deberá controlar su actuación, lo que servirá de base para periódicamente tomar la decisión de si se les renueva o no la confianza.

A partir de estas motivaciones, se realizó la propuesta del sistema y se desarrolló una prueba de concepto, lo que ha dado origen a las contribuciones que se recogen en el siguiente punto.

1.2. Principales contribuciones

Los objetivos concretos alcanzados y que se corresponden con la propuesta de tesis son los siguientes:

- Revisión bibliográfica de los modelos de confianza, criptografía ligera y seguridad en sistemas de Identificación por Radiofrecuencia (RFID).
- Recopilación de normativa relacionada con la trazabilidad alimentaria.
- Propuesta de un sistema que permite mediante una única operación criptográfica comprobar la validez de los datos de trazabilidad incluidos en una etiqueta RFID, basados en la identidad digital del producto.
- Realización de un prototipo del sistema, que ha servido para comprobar sus prestaciones y su compatibilidad con la cadena de producción de un matadero.
- Reflexionar sobre las mejoras relativas a la seguridad de los sistemas RFID que aporta el modelo propuesto.

1.3. Plan de trabajo y metodología

El plan de trabajo ha constado de las siguientes fases, ordenadas cronológicamente:

1. Revisión bibliográfica.
2. Definición del modelo de confianza.
3. Diseño de módulo de seguridad integrable en sistema de trazabilidad RFID.
4. Búsqueda de parámetros criptográficos óptimos.
5. Desarrollo del prototipo.
6. Evaluación del sistema en prototipo.
7. Conclusiones.

La primera parte del trabajo fue una revisión bibliográfica sobre los sistemas de identidad digital (definiciones, modelos de confianza y modelos de gestión de la identidad), trazabilidad, tecnología RFID y firmas agregadas.

A continuación se procedió a definir el sistema, en primer lugar enunciando el planteamiento teórico y posteriormente describiendo la prueba de concepto realizada. Una parte muy importante fue el estudio y selección de los criptosistemas más adecuados para trabajar con etiquetas de ultra-bajo coste, así como la selección de los parámetros de la firma electrónica que permiten compatibilizar los requisitos de seguridad, velocidad de proceso y escasez de recursos hardware.

Respecto a la metodología, se ha utilizado una combinación de dos métodos: el desarrollo en cascada [ROYCE1987] y el desarrollo con prototipación. El uso de estas dos metodologías de forma conjunta permite que se complementen y subsanen en gran medida las carencias que presentan por separado.

1.4. Estructura de la memoria de tesis

La memoria de tesis se ha estructurado en cinco capítulos, el primero de los cuales es esta introducción.

En el segundo capítulo se presenta una revisión bibliográfica, tanto de los aspectos conceptuales (identidad, confianza, reputación y gestión de la identidad) como de los aspectos más relacionados con las tecnologías utilizadas (trazabilidad, identificación por radiofrecuencia y firmas agregadas).

En el capítulo tercero se expone el sistema propuesto, incidiendo en sus diferentes aspectos, tanto el planteamiento teórico como su aplicación en una prueba de concepto, estudiando el sistema de relaciones de confianza, de gestión de la identidad, de seguridad, de provisión de certificación de calidad y el flujo de comunicaciones.

El cuarto capítulo, tras una descripción general del sistema, se centra en enunciar los requisitos de un caso de explotación real, y los diversos ajustes que ello conlleva. También se presenta la aplicación desarrollada y las diversas pruebas realizadas para elegir los parámetros criptográficos adecuados, así como la descripción del sistema prototipado. Se concluye este apartado con una reflexión de la contribución del sistema propuesto a la seguridad.

Por último, en el capítulo quinto, se presentan las conclusiones y se esbozan unas líneas futuras de investigación.

También se adjuntan cuatro anexos que completan la información referida en algunos apartados: un glosario sobre trazabilidad y otro sobre normativa y estándares RFID, un tercero sobre criptografía ligera en RFID y un cuarto y último sobre normativa de trazabilidad y seguridad alimentaria.

Para facilitar la consulta de las referencias bibliográficas, éstas se han ubicado al final del documento.

2. Revisión bibliográfica y estado del arte

Dado que el objetivo de este trabajo es desarrollar un sistema de identidad digital, con el que poder implementar un método de trazabilidad electrónica, desarrollado sobre un sistema RFID, en este capítulo se presenta una revisión de los conceptos relacionados con la identidad digital y la confianza. Sobre este concepto se implementará un sistema confiable de trazabilidad, aplicable a cualquier entorno productivo, y que será soportado por una PKI que utilizará certificados de claves para firmas múltiples, los cuales serán almacenados en una etiqueta RFID. Por lo tanto, es obligado revisar el estado del arte de todos estos conceptos, trabajo que se va a recoger en el resto del capítulo.

Este estado del arte se ha dividido en dos partes claramente diferenciadas. En la primera parte se engloba todo lo relacionado con el estudio teórico del concepto de identidad y los aspectos relativos a la provisión de identidad mediante atributos confiables, y en la segunda parte las cuestiones y herramientas relacionadas con su implementación en un sistema de trazabilidad.

Cada uno de los apartados incluye tanto una introducción al tema como una revisión bibliográfica que refleja el estado del arte en los diferentes ámbitos.

2.1. Planteamiento teórico: Sistemas de identidad digital

Siempre que una persona entra a formar parte de una comunidad con la que va a relacionarse, es necesario que se presente, es decir que se dé a conocer, para que los demás miembros de la comunidad puedan relacionarse con ella, asociarle un nombre, unos atributos y una reputación, o lo que es lo mismo: una identidad. En algunos entornos y circunstancias, se necesita que además se muestre algún tipo de credencial para que el resto de miembros puedan tomar como cierta dicha identidad, y asignar un grado de confianza a sus informaciones.

En el caso de la identidad digital, cuando una entidad (elementos activos del sistema) se quiere representar en una comunidad (ya sea un sistema de información, una red, etc…), esta representación se realiza incorporando a dicha entidad a una base de datos de usuarios, en la que también se le asigna un rol con una serie de privilegios y normalmente algún tipo de contraseña o mecanismo para que pueda autenticarse. Se entiende por entidad cualquier persona[2] o cosa que pueda ser caracterizada por sus atributos [MODINIS2005][RANNENBERG2009]. Por tanto, esta definición también

[2] *Física o jurídica*

engloba instituciones, empresas, máquinas, etc. Trabajos como [SUCH2011] amplían el concepto que se acaba de presentar de entidad, con el de "entidad software" que engloba agentes inteligentes, organizaciones virtuales, etc.

En el resto de este apartado se van a presentar diversos aspectos que se deben tener en cuenta cuando se hable de una identidad digital, como son los modelos de confianza y reputación y los modelos de gestión de la identidad.

Antes de continuar, debido a los diversos usos e implementaciones que hay de sistemas de identidad digital y métodos de gestión, conviene aportar una serie de definiciones, ya que a veces dada la utilización de los mismos términos en diversos ámbitos, se pierde su matiz y puede llevar a ciertas confusiones.

2.1.1. Identidad, autenticación y autorización.

En este punto se van a exponer las definiciones relacionadas con identidad, autenticación y autorización, así como su relación con el sistema planteado en esta tesis. La definición de los conceptos mostrados a continuación es importante, ya que muchas veces el concepto que tenemos asociado a los términos está condicionado inconscientemente por su uso en los sistemas tradicionales "basados en papel" que históricamente han soportado los procesos de identidad [CAMP2004].

- **Identidad:**

  1. Conjunto de atributos permanentes o temporales de larga duración asociados a una entidad [CAMP2004].
  2. Representación de una entidad en un contexto determinado [JØSANG2007] y consta de identificadores y credenciales de los usuarios.
  3. Es la representación, pruebas y credenciales de una entidad usuario la cual es asociada en un contexto determinado y es utilizada por aplicaciones y servicios para distinguir unos usuarios de otros y proporcionar diferentes privilegios a diferentes usuarios [CAO2010].

- **Identidad de una entidad:** en [SUCH2011] se define la identidad de una entidad $\boldsymbol{e}$ como $ב_e = \bigcup_j I_e^j$. La identidad $ב_e$ de la entidad $\boldsymbol{e}$ es la unión

de todas las identidades parciales I_e^j de $\boldsymbol{e}$ (la definición de identidad parcial se muestra a continuación).

- **Identidad parcial:** algunos autores se refieren a la identidad parcial como un subconjunto del total de atributos que posee una entidad [DAMIANI2003]. En [SUCH2011] se define formalmente identidad parcial como: "Dado un conjunto finito de atributos $A = \{a_1, \dots, a_n\}$ cada uno de ellos con un dominio finito $V_{a_i} = \{V_1, \dots, V_k\}$, un conjunto de entidades E y la entidad $\boldsymbol{e} \in E$, una **identidad parcial** de la entidad $\boldsymbol{e}$ es el vector $I_e = (i_1, \dots, i_n)$, que satisface que $i_j \in V_{a_j}$ y $\forall d \in E \backslash \{\boldsymbol{e}\} \Rightarrow I_d \neq I_e$. El conjunto de atributos A, el conjunto de valores para cada atributo a indicado como V_a y el conjunto de entidades E dependen del contexto. Por tanto, una **identidad parcial** I_e de una entidad $\boldsymbol{e} \in E$ es suficiente para identificar la entidad $\boldsymbol{e}$ dentro del conjunto E considerando A y V_a". Aunque cada identidad parcial normalmente identifica a la entidad en un contexto específico o rol, la misma identidad parcial puede identificar a la entidad en diferentes contextos. En la siguiente figura, basada en una figura de [SUCH2011], se muestra un esquema ilustrativo del concepto de identidad e identidad parcial.

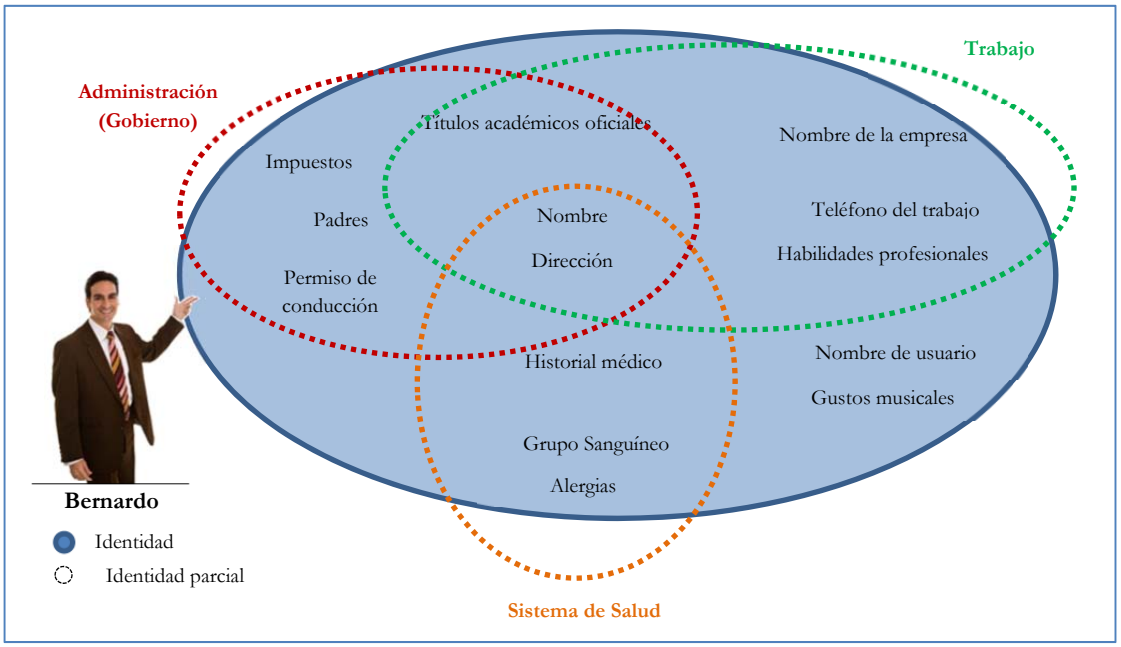

Fig. 2-1. Identidad vs Identidad parcial.

- **Identidad digital:** según [LINDEN2009] es una abstracción de un individuo en un sistema de información.

- **Identificador:** atributo o conjunto de atributos que identifican de manera única a personas, lugares o cosas en el contexto de un espacio de nombres específicos (cada espacio de nombres depende de una autoridad que lo controla y es la responsable de mantener que los identificadores sean únicos en ese espacio) [CAMP2004].

- **Identificador personal:** identificadores persistentes asociados con individuos humanos y atributos que son difíciles o imposibles de cambiar, como por ejemplo la fecha de nacimiento de una persona o su código genético [CAMP2004].

- **Identificación:** Asociación de un identificador personal con una persona que presenta ciertos atributos [CAMP2004].

- **Atributo:** característica asociada con una entidad, como ente individual. Pueden ser permanentes (por ejemplo: fecha de nacimiento, color de los ojos,…) o temporales de larga duración (por ejemplo el número de afiliación a la seguridad social) [CAMP2004][RANNENBERG2009].

Hasta aquí se han visto una serie de definiciones relativas a la identidad digital. Como se ha podido apreciar, están fuertemente orientadas a que el objeto de la identificación sean personas. Sin embargo, en esta tesis la identidad digital se contempla desde un punto de vista general, que permite incluso su aplicación a productos manufacturados. Además de suponer la abstracción del objeto en un sistema de información, esta identidad digital de los productos, se va materializar en un identificador, un elemento tangible que los va a acompañar físicamente y además también poseerá una vinculación lógica en el sistema de información. Adicionalmente a los atributos que se vayan incorporando a la identidad digital, también se recopilará información sobre los agentes que han comprobado e introducido dichos atributos en el sistema, de modo que también habrá identificadores de los agentes implicados, y el sistema tendrá cuantificado su nivel de confianza.

Una vez que se ha definido lo que se entiende en este trabajo por identidad digital, se van a mostrar una serie de definiciones relacionadas con la autenticación.

- **Autenticación:** Es una prueba de un atributo. Normalmente la autenticación se basa en [CRANOR2005]:

    - Algo que la entidad "sabe" (Ej. una contraseña) o es "capaz de reconocer" (Ej. una cara).
    - Algo que la entidad tiene (Ej. llaves, tarjetas inteligentes,…).
    - Algo que la entidad es (Ej. huella dactilar) o una característica típica de su comportamiento (Ej. forma de hablar).

  Estos métodos de autenticación, sobre todo el último, son aplicables principalmente cuando una máquina debe autenticar a un humano. Cuando la autenticación es entre máquinas, existe un método denominado autenticación fuerte, basado en el uso de técnicas y herramientas criptográficas.

- **Autenticación de identidad:** Asociación entre una entidad y un identificador [CAMP2004].

- **Autenticación de atributo:** Asociación entre una entidad y un atributo [CAMP2004].

Una vez expuestas las definiciones, se puede concretar que el sistema propuesto insertará en la identidad digital del producto un atributo que será avalado por una firma digital. Esta firma digital será un método de autenticación fuerte que permitirá autenticar tanto el producto (sólo los productos legítimos serán firmados por agentes de control autorizados) como a los agentes de control (ya que sólo si están autorizados podrán firmar el atributo). En la frase anterior se ha introducido un concepto no menos importante en el proceso, como es la autorización y el control de acceso, que a continuación se pasa a definir.

- **Autorización:** decisión de permitir una acción particular basada en un identificador o en un atributo. En sistemas de información la autorización suele estar ligada al concepto de **control de acceso**, es decir, decidir y auditar quién tiene acceso a qué dentro de un sistema. Tradicionalmente, desde los años 60 [LAMPSON1969], la forma de representar los permisos o autorizaciones en un sistema ha sido una matriz, en cuyas filas estaban los usuarios del sistema y en las columnas los objetos (o recursos) sobre los que podían (o no) actuar los usuarios [ANDERSON2008].

En el sistema propuesto, sólo los usuarios autorizados podrán introducir los atributos en la identidad digital de los productos. Los dos sistemas de autorización más importantes son los basados en roles (los más utilizados en la actualidad) y los basados en atributos. Ambos sistemas se definen a continuación.

- **Autorización basada en Roles *(RBAC, Role-Based Access Control)*:** en organizaciones con muchos usuarios (que además pueden darse de alta, de baja o cambiar sus atributos) y muchos objetos sobre los que controlar el acceso, la utilización de matrices de control de acceso era inviable. Por ello, en los años 90 surgió el sistema de acceso basado en roles, entendiendo el rol como un nivel de abstracción entre los sujetos y las acciones que estos pueden hacer con los objetos [LINDEN2009]. El término RBAC fue introducido en 1992 en [FERRAIOLO1992], y la publicación de la familia del modelo RBAC fue en 1996 [SANDHU1996]. En RBAC, cada usuario tiene uno o varios roles, y cada uno de estos roles otorga una serie de privilegios (es decir, autorizaciones o permisos) sobre un determinado objeto (que puede ser un servicio, un archivo, etc.). Para ampliar este tema se recomienda la lectura de [FUCHS2011].

- **Control de acceso basado en atributos *(ABAC, Attribute-Bassed Access Control)*:** los permisos dependen de algunos de los atributos del usuario, servicio o entorno [YUAN2005].

2.1.2. Confianza y reputación

En este apartado se van a presentar los conceptos de confianza y reputación. Ambos conceptos son muy importantes en esta tesis, ya que posteriormente se propondrá un sistema de confianza basado en la reputación de los agentes de control que permitirá de forma autónoma y automática establecer un nivel de confianza en un agente de control que evolucionará a lo largo del tiempo, según el número de errores del operario y su frecuencia. Para abordar el estudio de estos dos conceptos se ha utilizado el enfoque propuesto por Sabater y Sierra en [SABATER2005].

Cuando se presentan estos términos, es habitual en la bibliografía tratarlos desde diferentes perspectivas. Las más comunes suelen ser desde la sicología [BROMLEY1993, KARLINS1970], la sociología [BUSKENS1998], la filosofía

[HUME1739, PLATON2009] y la economía [CELENTANI1996, MARIMON2000].

- **Confianza:**
  1. Según Gambetta [GAMBETTA1988], es "*la probabilidad subjetiva por la cual una persona, A, espera que otra persona, B, realice una acción determinada de la cual depende su bienestar*". De forma general, entendemos que la confianza es la expectativa que tiene A de que B haga algo que le beneficie.
  2. **"***Medida acerca de la certeza que se tiene en que otro agente será capaz de ejecutar eficientemente una determinada acción, teniendo en cuenta su propio conocimiento*" [CABALLERO2008]. Esta definición, dado su carácter generalista, será la que utilizaremos como referencia (aunque cite explícitamente a un agente, realmente puede entenderse para hacer la definición más extensa agente como entidad que posee cierta información).

Respecto a reputación, aunque también existen múltiples definiciones, se ha optado por presentar dos definiciones que tienen un amplio campo de aplicación.

- **Reputación:**
  1. Es una evaluación basada en la historia de interacciones u observaciones de una entidad, ya sean realizadas directamente por el evaluador o transmitidas por un testigo [JØSANG2007].
  2. Certeza que un agente tiene sobre el comportamiento de otro, compuesta a partir del conocimiento que es capaz de extraer de las relaciones con el resto de agentes, ya sea por el análisis de la red de relaciones sociales como por la información suministrada por otros" [CABALLERO2008].

Como se ha señalado, se utilizará el término de confianza como una medida acerca de la certeza que se tiene en que un agente de control ejecutará eficientemente el control e introducción en el sistema del atributo del que sea responsable, teniendo en cuenta el número de fallos en su tarea a lo largo del tiempo. Entenderemos reputación, como un nivel cuantitativo resultado de una evaluación de la historia de errores de un agente, y que se relacionará directamente con la confianza.

2.1.3. Modelos de confianza y reputación

Tomando la definición dada en [CABALLERO2008], se puede referir que los modelos de confianza y reputación tienen como principal objetivo aportar mecanismos que apoyen la toma de decisiones de las partes integrantes de un sistema para su interacción, dando respuestas a problemas claves como: ¿Con quién, cuándo y cómo interactuar? Concretando un poco más, según [CABALLERO2008] la mayoría de los modelos tratan de resolver un conjunto de problemas comunes entre los que destacan:

- ¿Cómo saber con quién interactuar? Suele ser el objetivo fundamental de los sistemas de confianza y reputación.
- ¿Cómo se evalúa una acción y cómo se refleja en el modelo? Al finalizar cada acción, debe actualizarse el modelo para contemplar dicho suceso de cara a futuras interacciones, teniendo en cuenta sobre todo la calidad de la solución y la satisfacción del usuario.
- ¿Cómo tratar la información proporcionada por otros? Como no todas las entidades tendrán el mismo nivel de confianza, se deberá tener esto en cuenta a la hora de procesar la información. También es importante poder combinar información de diversas procedencias. Además será deseable disponer de mecanismos que permitan detectar comportamientos fraudulentos o maliciosos de los agentes.

En [BECERRA2007] se plantea que confianza y reputación pueden ser establecidas en base a cuatro atributos fundamentales: integridad, previsibilidad, competencias y motivación.

- **Integridad:** hace referencia a qué nivel de honradez posee una entidad integrante del sistema. Es uno de los atributos más utilizados en los modelos de confianza. En sistemas cooperativos (no competitivos) los agentes suelen ser honestos, pero en entornos competitivos los agentes pueden no responder a preguntas, o responder con información parcial o incluso falsa, por lo que son necesarios mecanismos de control que detecten este tipo de comportamientos [CABALLERO2009, HUYNH2006, PATEL2005, SABATER2001, TEACY2006, ZACHARIA1999].

- **Previsibilidad:** este atributo cuantifica la incertidumbre, es decir cuanto menor sea la incertidumbre sobre el futuro comportamiento de una entidad, mayor será su previsibilidad.

- **Competencias:** hace referencia a la capacidad que tiene una entidad (normalmente un agente) para realizar las tareas que se le encomienden dentro de un contexto determinado.

- **Motivación:** tiene que ver con el interés que tiene una entidad por completar una determinada tarea. Muchos modelos no la contemplan.

En el siguiente punto se presentan varias clasificaciones, que permitirán repasar estructuradamente algunos de los modelos más extendidos de confianza y reputación.

2.1.3.1. Parámetros para la clasificación de modelos de confianza

En este punto se presentan una serie de parámetros que permiten realizar una clasificación de los modelos de confianza, y que servirán para comprender mejor las particularidades y usos de algunos de ellos, que serán referenciados en este apartado.

La distinción más general sobre los modelos de confianza y reputación puede hacerse en base a la procedencia de la información. Así, si la información procede de la propia experiencia se hablará de modelos de confianza, mientras que cuando la información venga de terceros se hablará de modelos de reputación. También hay modelos en los que convergen ambas fuentes de información, denominados modelos de confianza y reputación.

Otro parámetro para clasificar los modelos, también muy general y frecuentemente utilizado, es la distinción de los modelos según las **teorías de base** utilizadas para construirlos, es decir según su modelo conceptual sea numérico o cognitivo:

- ***Modelo conceptual:***

  - *Modelos numéricos:* basados en teoría de juegos (*Game Theory, GT)* [GONZALEZ2010] o en otras aproximaciones probabilísticas

como la teoría de la información *(Information Theory)* [SHANNON1948].

- *Modelos cognitivos:* como se señala en [ESFANDIARI2001], en estos modelos la confianza y la reputación se construyen sobre las creencias subyacentes y son una función del grado de estas creencias. Por tanto, los estados mentales que llevan a creer en otro agente o asignar una reputación, así como las consecuencias mentales de la decisión y el acto de confiar en otro agente, son una parte esencial del modelo. En [PINYOL2011] se cita como ejemplos de este tipo de paradigma los modelos descritos en [CASTELFRANCHI1998] y [SABATER2006].

En [SABATER2005] se introduce la clasificación basada en las fuentes de información, permitiendo incluso establecer los valores de confianza en ellas:

- ***Fuentes de información:***

  - *Experiencias directas* (éstas son las fuentes más importantes y fiables para un modelo de confianza y reputación). Estas experiencias directas pueden venir de la relación directa con otra entidad (o agente) o de la observación de la interacción de otros miembros de la comunidad entre sí (en este caso se asume que existirá una cierta cantidad de ruido en la información).
  - *Información de testigos* (también denominada *información indirecta*). Es la que proviene de otros miembros de la comunidad. Es la más abundante, pero también es compleja de manejar debido a la falta de certeza que la rodea, así como a su posible manipulación por parte del testigo para su beneficio (por ejemplo, ocultando datos que pudieran perjudicarle).
  - *Información sociológica (redes de relaciones sociales).* Este conocimiento se basa en la relaciones sociales entre los agentes y el rol que los agentes desempeñan en la sociedad (o comunidad).
  - *Prejuicio.* Aunque mucho menos utilizado, el uso de prejuicio es otro método de cálculo para valores de confianza y reputación. El prejuicio es un mecanismo que permite asignar propiedades

(por ejemplo reputación) a un individuo, basado únicamente en símbolos que identifican al individuo como miembro de un grupo (por ejemplo llevar uniforme).

Finalmente, Becerra et al. en [BECERRA2007], propone una clasificación basada en cinco parámetros:

- ***Tipos de visibilidad:*** la confianza y la reputación de un individuo pueden tratarse como una **propiedad global de dominio público** compartida por todos los observadores o como una **propiedad subjetiva** valorada de manera particular por cada individuo, y que permanece en secreto. En el primer caso el valor de confianza o reputación se calcula en base a las opiniones de individuos que en el pasado han interactuado con el individuo que está siendo evaluado. Este valor es publicado para que sea accesible por todos los miembros de la comunidad, y actualizado cada vez que un miembro lleva a cabo la evaluación de un individuo. Es fundamental establecer métodos de control para evitar que el intercambio de información incompleta o falsa. En el segundo caso, se habla de la confianza o reputación de un individuo *x* desde el punto de vista del individuo *y*.

- ***Granularidad de los modelos:*** es evidente que la confianza y la reputación **dependen del contexto** (no confiamos igual en el médico cuando nos receta un medicamento que cuando nos recomienda una determinada película). Añadir a los modelos computacionales de confianza y reputación la posibilidad de manejar diferentes contextos tiene un coste en términos de complejidad y añade algunos efectos colaterales que no siempre son necesarios o deseables.

- ***Supuestos de comportamiento de los agentes:*** la base de esta clasificación es la capacidad para tratar con agentes que muestran diferentes grados de comportamiento fraudulento. Se definen 3 niveles:

  - Nivel 0. No se considera posible el comportamiento fraudulento.

  - Nivel 1. El modelo asume que los agentes pueden ocultar información, pero no mentir.

  - Nivel 2. El modelo tiene elementos específicos para tratar a los mentirosos.

- ***Tipo de información intercambiada:*** la base de esta clasificación es el tipo de información esperada por parte de los testigos. Hay dos grandes grupos:

  - Los que esperan información binaria (*booleana)*.

  - Los que esperan medidas continuas.

- ***Medida de la fiabilidad de la confianza o reputación:*** a veces es tan importante como el propio valor de reputación o confianza, la fiabilidad o la confianza que tenemos en ese valor.

En la Tabla 2-1, se presenta un resumen de todos los parámetros presentados. Aunque la clasificación es válida para modelos generales, está especialmente enfocada a modelos de confianza computacionales (los más numerosos):

• Modelo conceptual	Numéricos Cognitivos
• Fuentes de información	Experiencias Directas Información de Testigos Información Sociológica Utilización de prejuicios
• Tipos de visibilidad	Global Subjetiva
• Granularidad	Dependiente del contexto No dependiente del contexto
• Supuestos de comportamientos de los agentes	Nivel 0. No fraudulento Nivel 1. Pueden ocultar información Nivel 2. Pueden mentir
• Tipo de información intercambiada	
• Medida de la fiabilidad de la confianza o reputación	

Tabla 2-1. Resumen de clasificación de modelos.

Además de los parámetros que acabamos de exponer, existen otras clasificaciones como las propuestas por [BALKE2009] (centrada en un proceso de cinco etapas) o la presentada en [PINYOL2011] que permite clasificar los modelos más recientes, y está basada en cuatro parámetros:

- ***Confianza:*** desde el concepto de confianza social de [CASTELFRANCHI1998a], al de "*ocurrent and dispositional trust*" de [HERZIG] pasando por el modelo de decisiones estratégico-pragmáticas apuntado por [CONTE2002], los autores deducen que confianza implica decisión, y por tanto la confianza puede ser vista como un proceso de razonamiento práctico que va encaminado a la decisión de interactuar (o no) con alguien.

- ***Dimensión cognitiva:*** en este parámetro, los autores diferencian entre los modelos que tienen una clara representación de la confianza, reputación, etc. en términos de creencias, metas, deseos, intenciones,… y los que no la tienen.

    - Los modelos que tienen esta dimensión, describen explícitamente las actitudes epistémicas y motivacionales que son necesarias para que los agentes tengan confianza o hagan evaluaciones sociales. Los valores finales de confianza y reputación son tan importantes como la estructura que los soporta. Estos modelos suelen ser muy claros a nivel conceptual, pero tienen muchas carencias en aspectos computacionales.

        - Desde el punto de vista humano, esta dimensión permite un mejor entendimiento de los componentes internos de confianza y reputación, y una clara implicación de cara a las posibles decisiones finales.

        - Desde el punto de vista de los agentes *software*, esta dimensión dota a los agentes de una clara capacidad de explicar sus decisiones y razones sobre su propia estructura de confianza, haciendo posible el metarrazonamiento [CASTELFRANCHI 2007].

- Los que no poseen dimensión cognitiva, consideran al modelo como una "caja negra" que recibe una serie de entradas y emite como salida valores de confianza y reputación. Normalmente en el aspecto computacional están muy bien definidos y pueden expresarse con fórmulas analíticas.

- ***Procedimiento:*** normalmente, los modelos presentan una buena forma de representar y abordar la confianza y la reputación, pero no hay explicaciones sobre cómo han llegado a ello. Es muy común en los modelos cognitivos, centrados en sus componentes internos de confianza y reputación, pero no en cómo están construidos dichos componentes.

- ***Generalidad:*** los autores clasifican los modelos teniendo en cuenta si son de propósito general, o si por el contrario están enfocados para escenarios muy específicos.

A continuación se presentan algunos los principales modelos computacionales basados en agentes, en una tabla basada en [PINYOL2011]. Se han incluido sólo los de propósito general, excluyendo por tanto algunos como el de Abdul-Rahman et al. [ABDUL-RAHMAN2000], LIAR [MULLER2005], Regan y Cohen [REGAN2005], Ripperger [RIPPERGER1998], Sen y Sajja [SEN2002] y el de Yu y Singh [YU2002a, YU2002b, YU2003].

Modelo	Confianza	Dimensión Cognitiva	Procedimiento	Generalidad
Castelfranchi et al. [CASTELFRANCHI 1998]	+	+	-	+
AFRAS [CARBO2003]	-	-	+	+
Esfandiari et al. [ESFANDIARI2001]	-	-	+	+
FIRE [HUYNH2006]	*	-	+	+
ForTrust [HERZIG2010]	+	+	-	+
Marsh [MARSH1994]	+	-	-	+

Modelo	Confianza	Dimensión Cognitiva	Procedimiento	Generalidad
Mui et al. [MUI2002]	+	-	-	+
REGRET [SABATER2001]	*	-	+	+
Scichillo et al [SCHILLO1999, SCHILLO2000]	-	-	+	+
Sierra y Debenham [SIERRA2005]	+	-	+	+
BDI + Repage [PINYOL2012]	+	+	+	+

Tabla 2-2. Algunos modelos computacionales según la clasificación de 4 parámetros de Pinyol et al [PINYOL2011].

El valor "*" en el campo confianza de la Tabla indica que el modelo no explicita el mecanismo de decisión, y por tanto no se ajusta exactamente a la definición de confianza, pero se aproxima bastante, ya que permite finalmente realizar una decisión de con quién interactuar.

2.1.3.2. Clasificación de modelos según el tipo de control

Desde el punto de vista del tipo de control de los sistemas de confianza y reputación, podemos clasificar los sistemas como centralizados o descentralizados (también denominados distribuidos).

Los entornos centralizados, utilizados sobre todo en comercio electrónico, tienen unos mecanismos de confianza y reputación relativamente simples, caracterizados según [CABALLERO2008] por:

- Existencia de un nodo central, o alguna entidad institucional, que mantiene toda la información relativa a los indicadores de confianza, y se responsabiliza de la veracidad de dicha información.

- La información de confianza y reputación es ofrecida por el sistema.

- No existe un diálogo entre las partes del sistema para obtener los valores de reputación.

Los modelos en entornos de control descentralizado, son más complejos y presentan en general las siguientes características [CABALLERO2008] :

- No existe un elemento central que ofrezca métricas sobre el desempeño de los agentes.
- Cada elemento debe mantener actualizado su propio modelo sobre el comportamiento del resto de sus vecinos y de las relaciones con ellos.
- Se intercambia un gran volumen de información de reputación y confianza.
- Los valores de confianza y reputación se mantienen como información privada que en muchos casos se utiliza para obtener ventajas en las interacciones con otros.

En el apartado anterior se han presentado clasificaciones y un buen número de modelos, pero orientados a los sistemas descentralizados, y concretamente pensando en modelos computacionales para su implementación en agentes. Para el tipo de problema abordado en esta tesis, es decir, la interacción entre empresas que se conocen y que deben negociar físicamente sus condiciones de negocio, parecen más adecuados los modelos centralizados. Por ello a continuación, se van a describir brevemente algunos de estos modelos [PINYOL2011]:

- ***Modelos de reputación on-line.***
  Suelen utilizarse para comercio electrónico. Se basan en la posibilidad de que tras una transacción el comprador pueda opinar y calificar al vendedor. Al final el vendedor tiene una reputación (ya sea una puntuación, un color, un número de estrellas,…). Estos modelos están ideados para la interacción entre personas. Su principal problema es la falta de robustez, ya que no incorporan medidas de fiabilidad ni contramedidas para casos de información no completa o falsa.

- ***Sporas e Histos*** [ZACHARIA1999]**.**
  Es una evolución natural de los modelos de reputación *on-line*. El planteamiento es básicamente similar, pero en este caso sólo se tienen en cuenta las valoraciones más recientes. Además, su algoritmo se encarga de que para los vendedores con una buena reputación los cambios sean pequeños, mientras que para los vendedores con poca reputación los cambios de valoración sean mucho mayores. También incorpora una cuantificación de la fiabilidad de los usuarios.

- *Sporas,* según se indica en [CABALLERO2008] es un mecanismo de reputación simple que puede ser implementado sin tener en cuenta el número de interacciones que se evalúen, ya que sólo se tiene en cuenta la más reciente. Cada nuevo agente, empieza con reputación muy baja y se va actualizando con las opiniones de otros agentes. Tiene un único valor de reputación global para cada agente e incorpora medidas de fiabilidad basada en la desviación estándar de los valores de reputación. Para evitar complicidades entre dos agentes, incluye la condición de que cada par de agentes sólo se pueden evaluar una vez, aunque no controla las complicidades entre más de dos agentes (lo que sí hace *Histos*).

- *Histos*, como señala Caballero en [CABALLERO2008] es más complejo que el anterior, ya que sí toma en consideración gran cantidad de información relativa a las evaluaciones que un agente hace de otro al interactuar, aunque sólo tiene en cuenta las experiencias más recientes. Resuelve el problema de la falta de personalización de los valores de reputación, considerándola una propiedad intrínseca a la relación entre dos agentes. Para ello construye un grafo cuyos nodos representan los agentes y los arcos la evaluación más reciente que tiene un agente sobre otro. El nodo de origen del arco es el nodo que evalúa, y el de destino el evaluado. Es similar a la representación *TrustNet* [SCHILLO2000].

- ***Carter et al*** [CARTER2002]**.**
  Basado en la idea de que la reputación de un agente es el grado de cumplimiento de los roles que le asigna la sociedad [SABATER2005]. Cada sociedad define una serie de roles que se pueden desempeñar, y la reputación de cada participante es el resultado de una agregación ponderada del cumplimiento alcanzado por el agente en cada rol. Es difícil de calcular y depende del contexto de cada sociedad, por lo que es necesaria una autoridad de control que realice el cálculo y controle las transacciones.

- ***Kuhlen*** [KUHLEN1999]**.**
  Plantea que una autoridad de control evalúe objetivamente ciertos estándares de calidad, y otorgue un sello cuando se cumplan ciertos requisitos.

- ***Dirichet reputation systems*** [JØSANG2007].
  Este tipo de sistemas trabaja muy bien en entornos centralizados, donde los usuarios son calificados en base a un conjunto discreto y finito de valoraciones o categorías. Estos modelos tienen la capacidad de dar una distribución de probabilidad dentro de un conjunto ordenado, representando la probabilidad de que un agente actúe según lo esperado dentro de cada una de las categorías.
  Los modelos de esta familia, utilizan una distribución de probabilidad de Dirichet: una distribución bayesiana polinomial. La idea es aproximar el conjunto de valoraciones de los usuarios a la distribución de Dirichet apropiada y luego extrapolar el valor de cada categoría [PINYOL2011].

2.1.4. Modelos de sistemas de gestión de la identidad

La gestión de la identidad es un tema muy importante desde que los ordenadores comenzaron a almacenar y manejar datos personales y confidenciales. Está claro, que cualquier sistema que trabaje con datos personales deberá ofrecer garantías de que sólo las personas autorizadas podrán acceder o modificar la información. Un ejemplo sería un banco, donde es imprescindible que tanto el acceso a la información como su modificación (por ejemplo el saldo de una cuenta) estén restringidos y auditados.

Antes de la popularización de las redes de computadores o Internet, los usuarios ya distinguían sus procesos y programas de los de otros usuarios mediante el uso de contraseñas. Desde este estado inicial, la situación ha cambiado mucho y actualmente es frecuente que un usuario tenga multitud de cuentas, cada una con su identificador de usuario y su contraseña, en multitud de servicios. Por ejemplo es habitual que un usuario tenga cuentas en su lugar de trabajo, en *gmail*, en *Facebook*, en *twitter*, en comercios electrónicos, en bancos,… y todas ellas distintas. Esta situación límite, en la que la cantidad de parejas usuario-contraseña llega a ser inmanejable para el usuario, es cada vez más habitual.

Por todo lo anterior, la gestión de todo este complejo entramado de usuarios y claves, hace conveniente y deseable el planteamiento de sistemas que faciliten la gestión de estas identidades (y en el caso de Internet la utilización de menos duplas de identificación, es decir que con una única pareja usuario-contraseña se tenga acceso a diversos servicios).

Hay tres motivaciones importantes para invertir en sistemas de gestión de identidad: seguridad de la información, eficiencia y nuevas oportunidades de negocio (sobre todo para empresas que trabajan en el comercio electrónico).

Como señala [LINDEN2009], el objetivo de la gestión de identidad puede abordarse desde dos perspectivas:

- Desde el punto de vista técnico: asegurar que los usuarios finales sólo podrán realizar las acciones para las que han sido autorizados.

- Desde el punto de vista jurídico: asegurar que se pueda responsabilizar a una persona de las acciones realizadas bajo su identidad autenticada.

Además, otras tareas importantes relacionadas con la gestión de identidad son la administración de identidades y los procesos de auditoría sobre dichas gestiones. Teniendo en cuenta que el sistema de confianza queremos que sea operativo entre diferentes entes y en diversos entornos, se debe tener en consideración la forma en la que se gestionarán las credenciales de los participantes en los procesos. A continuación se presenta una definición tanto de gestión de la identidad como de otros conceptos relacionados, como proveedor de servicio, proveedor de identidad y usuario.

- **Gestión de la identidad *(IdM, Identity Management):***
  1. Sistema y estructura utilizados en ordenadores o sistemas de comunicación para controlar la identidad [DABROWSKI2008]. Incluye relaciones de confianza, construidas sobre la identidad, verificación de autenticidad de entidades, autorización de control de acceso, transferencia segura de atributos de identidad, gestión del ciclo de vida de la identidad, administración del flujo de trabajo en el intercambio de identidades, y federación de entidades entre diferentes dominios y delegaciones dinámicas de confianza.
  2. Sistema integrado de procesos de negocio, políticas y tecnologías que permiten a las organizaciones controlar el acceso de los

usuarios a aplicaciones en línea y recursos, a la vez que se protege la información personal confidencial y la información de empresa de usuarios no autorizados [ACSQHC2010].

3. Recurso de control de acceso y gestión de la información de identidad implementada con nuevas tecnologías, cuyo objetivo es el ahorro de costes de gestión de usuarios y sus identidades, atributos y privilegios de acceso para mejorar la productividad y la seguridad [LEE2003].
4. Infraestructura de autenticación de identidad y gestión de autorizaciones y permisos desarrollada con nuevas tecnologías para reducir los costes de gestión de identidades y privilegios de acceso de los usuarios, con el objetivo de mejorar la seguridad y la privacidad, la compartición de información, la eficiencia en el trabajo y la seguridad [CHANG2009].
5. Políticas, reglas, métodos y sistemas que implementan la autentificación de la identidad, gestión de permisos, control de acceso y operaciones de auditoría basadas en la identidad digital [CAO2010].

- **Proveedor de Servicio (SP, *Service Provider)*:** en los sistemas de gestión de identidad, se define como proveedor de servicio a la entidad que se encarga de proporcionar un servicio determinado a un usuario (comercio electrónico, banca electrónica, acceso a información, etc. [CAO2010].

- **Proveedor de Identidad (IdP, *Identity Provider):*** según [CAO2010] es una entidad que constituye el núcleo de los sistemas de gestión de identidad. Provee diversos niveles de confianza a diferentes tipos de usuarios. Tiene dos funciones principales:

  - ***Implementación de servicios de identidad*:** registro de usuarios, verificación de la identidad real del usuario antes de confirmar el registro y almacenamiento de los datos de identidad del usuario.

  - ***Procesar las solicitudes*** tanto del proveedor de servicio como de los usuarios para su autenticación.

- **Usuario:** es el "cliente" de los proveedores de servicio y de identidad. Debe tener una identidad válida si quiere utilizar los servicios. Puede ser una empresa, una organización, una persona, una entidad virtual de software, etc. [CAO2010].

Una vez mostradas las definiciones sobre los diferentes agentes, a continuación se van a presentar algunas clasificaciones para estos sistemas. En [MIYATA2006] y [AHN2007] se proponen clasificaciones para los sistemas de gestión de la identidad, mientras que en [JØSANG2005] se propone una clasificación para los sistemas proveedores de identidad.

Atendiendo a los servicios, los tipos de proveedores de servicio (SP), el almacenamiento de identidades, los tipos de proveedores de identidad (IdP) y el control del usuario sobre los aspectos de protección de identidad y protección de la privacidad, en [CAO2010] se propone una clasificación de sistemas de gestión de la identidad, con tres tipos de modelos: modelo aislado, modelo centralizado y modelo federado.

- **Modelo aislado**

  En el modelo aislado el proveedor de servicio actúa también como proveedor de identidad y como proveedor de atributos, es decir, toda la información relativa a la identidad y todas las operaciones realizadas por los usuarios son almacenadas en un único servidor. Por tanto, las operaciones relativas a identificador único de identidad, modificación, supresión, autenticación y autorización están implementadas en el propio proveedor de servicios.

  La principal ventaja de este modelo es su sencillez, y su principal inconveniente es que no es escalable. Conforme crece el número de servicios que utiliza el usuario, éste debe manejar un gran número de claves y credenciales. Además, esto último hace que al final el sistema sea poco utilizable, y propicie frecuentes olvidos de contraseñas y pérdidas de credenciales, lo que supone un coste añadido para el proveedor de servicios.

  Cada usuario tiene credenciales separadas para cada identidad, asociadas a contraseñas o parámetros biométricos, como se representa en la Fig. 2-2.

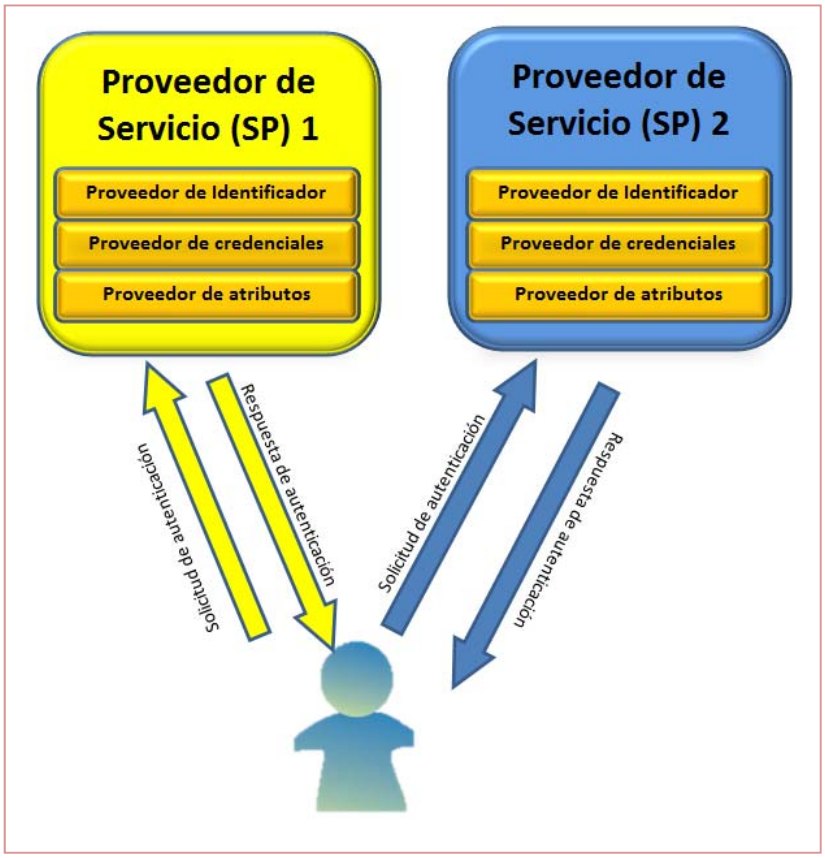

Fig. 2-2. Modelo aislado de Gestión de Identidad

- **Modelo centralizado**

El modelo centralizado se implementa como un sistema cliente-servidor. La información de identidad del usuario y la autenticación se implementan en el mismo servidor, denominado "Proveedor de identidad" (IdP, *Identity Provider).*

Al margen del proveedor de identidad, está el proveedor de servicio que únicamente solicita la autenticación del usuario al proveedor de identidad, y una vez autenticado el usuario procede a prestarle el servicio demandado. Por tanto, el proveedor de servicio no almacena ninguna información de identidad del usuario ni realiza la autenticación.

Normalmente varios proveedores de servicio utilizan un proveedor de identidad común para todos. En la Fig. 2-3 se representa este esquema.

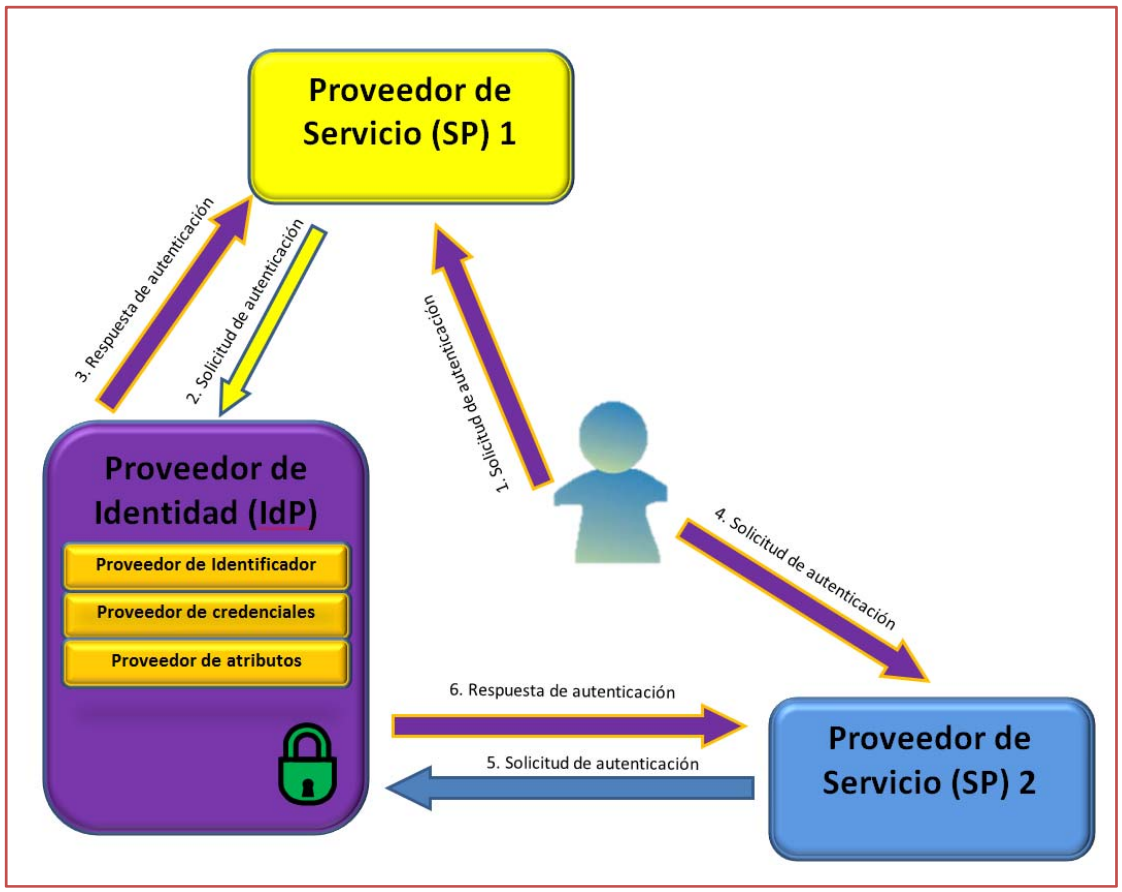

Fig. 2-3. Modelo Centralizado de Gestión de Identidad

Aunque este modelo puede implementarse de múltiples maneras, las tres más importantes son [JØSANG2005]: el modelo de identificador común, el modelo de metaidentificador y el modelo SSO (*Single Sign On*).

Hay muchos sistemas implementados con el modelo centralizado, como por ejemplo los de Infraestructura de Clave Pública (PKI , *Public Key Infraestructure)*, Kerberos [3] y CAS [4] (*Central Authentication Service*).

Este modelo es adecuado para gestionar identidades de muchos usuarios que además accedan a múltiples proveedores de servicio, pero presenta algunos inconvenientes, sobre todo derivados del almacenamiento de todas las identidades en un único proveedor de identidad. El principal inconveniente se refiere a la protección de la privacidad. Este modelo tampoco soporta la delegación de privilegios y el acceso cruzado a dominios.

[3] *http://web.mit.edu/kerberos*
[4] *http://www.jasig.org/cas*

- **Modelo federado**

La idea del modelo federado es que aunque los usuarios estén en diferentes dominios, aparentemente exista un dominio único. Este modelo está basado en el intercambio de datos entre los diferentes dominios reales, que se integran en el dominio virtual único.

En [CAO2010] lo definen como un conjunto de acuerdos, normas, estándares y tecnologías que permiten a un grupo de proveedores de servicios reconocer identidades de usuario de otros proveedores de servicio dentro de un dominio federado de confianza. De este modo, una vez que un usuario se ha autenticado en un dominio, el resto de dominios federados lo consideran autenticado, y por tanto puede acceder a cualquier otro dominio de la federación de forma cómoda y segura sin necesidad de repetir el proceso de autenticación.

En este modelo se establece una relación entre los diferentes identificadores que posee un usuario en diferentes dominios. Esta operación permite que los usuarios autenticados en un dominio puedan acceder a cualquier otro de los federados. Es decir, los usuarios pueden seguir manteniendo identificadores separados para cada proveedor de servicio, siendo posible el acceso al resto de dominios con cualquiera de ellos.

Los sistemas de autenticación reducida (SSO, *Single Sign On)*, que permiten al usuario mediante un único identificador acceder a varios sistemas, son diferentes de los sistemas centralizados. En los federados sí está soportado el *cross domain SSO*, es decir el SSO a través de múltiples dominios, mientras que en los centralizados sólo soportan el SSO en un único dominio.

En la Fig. 2-4 se muestra un esquema del modelo. En el área de color rojo se han encerrado todos los proveedores de servicio, es decir, todo el conjunto de dominios federados, que puede ser considerado como un proveedor de servicio único virtual. Como se representa, todos los identificadores y credenciales del usuario pueden funcionar virtualmente como una identidad global. Cada proveedor de servicio puede tener y gestionar su propia base de datos de identidades. Además, los proveedores de identidad tienen únicamente una base de datos de identidad limitada a los requerimientos mínimos de información para el correcto funcionamiento del sistema federado.

El sistema es transparente al usuario, y actúa como si fuera un único proveedor de servicio global.

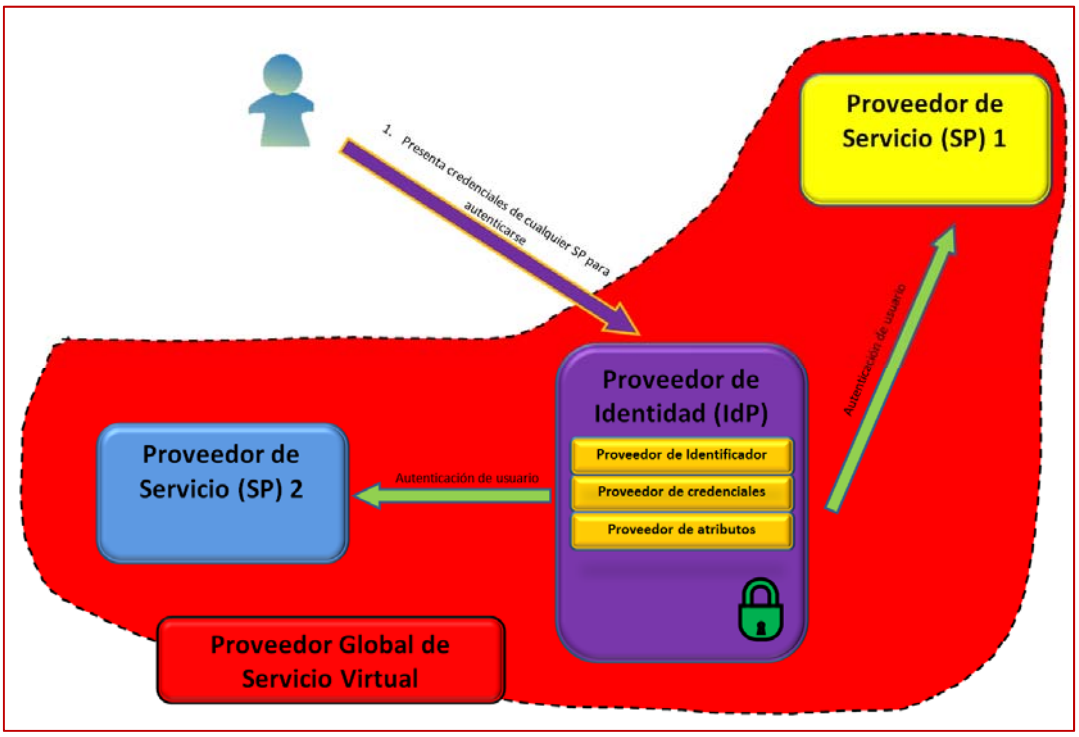

Fig. 2-4. Modelo Federado de Gestión de Identidad

En [CAO2010] se citan algunos protocolos, estándares y sistemas para este modelo federado, como SAML[5] (*Security Assertion Markup Language*) desarrollado por los servicios de seguridad del comité técnico de la organización para el avance de los estándares de información estructurada (OASIS[6], *Organization for the Advancement of Structured Information Standards)*, *WS-Federation*, *Liberty Alliance Framework*[7], *Shibboleth*[8] u OpenID[9] [RECORDON2006].

En cuanto a los defectos del sistema, como señala Bertino [BERTINO2009], destacan los relacionados con el ciclo de vida de la identidad (creación, utilización, modificación y revocación), donde puede haber problemas de seguridad y gestión de la privacidad, al tener que sincronizar varios proveedores de identidad.

[5] *https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security*
[6] *http://www.oasis-open.org*
[7] *http://kantarainitiative.org/*
[8] *http://shibboleth.net/*
[9] *http://openid.net/*

Hasta aquí la clasificación basada en la concentración de los proveedores de servicio, que es con diferencia la más ampliamente utilizada. Respecto a la clasificación basada en paradigmas, [CAO2010] propone la siguiente: centrado en la red, centrado en el servicio y centrado en el usuario. Esta clasificación, aunque aporta un interesante punto de vista, está menos extendida que la que acabamos de ver.

- **Centrado en la red:**

  - En este modelo la creación de identidades, su gestión y su eliminación no tiene nada que ver con el acceso o privilegios. Cada sistema de gestión de la identidad trabaja como una entidad única con unos usuarios fijos y unos recursos comunes.

  - Nace en los primeros pasos de los sistemas de gestión de identidad y fue utilizado en los comienzos de las redes de computadores, cuando aparecieron los primeros recursos de red compartidos.

  - Como ejemplo se puede citar el sistema inicial de gestión de dominios de Microsoft Windows, gestionado por unos administradores y unos servidores de control de dominio.

  - Con la evolución de los sistemas, este modelo cayó en desuso, debido sobre todo a que no era capaz de manejar atributos ni formar sistemas federados.

- **Centrado en el servicio:**

  - Este modelo está basado en la incorporación de diferentes servicios, de diferentes proveedores pertenecientes a distintos dominios. El sistema permite la inclusión dinámica de nuevos servicios.

  - Para el usuario todo debe ser transparente. Ejemplo: una vez autenticado, si hay un nuevo programa de mensajería instantánea, el usuario podrá elegirlo y automáticamente el sistema deberá entender esta acción como que el usuario delega los permisos de acceso que tenía su anterior cliente de

mensajería instantánea en el nuevo (y los retira del anterior hasta nueva orden).

- Este modelo es muy complejo y ambicioso, ya que podría integrar todos los recursos *on-line* de una organización, incluyendo ordenadores, dispositivos de red, servidores, portales, contenidos, aplicaciones, productos, usos de credenciales, agendas de direcciones, autorizaciones o agendas de números de teléfono.

- Tiene dos retos fundamentales para resolver:

  - es muy difícil integrar los servicios de diferentes proveedores y diferentes dominios, sobre todo porque normalmente tienen distintos mecanismos de control de acceso y niveles de confianza.

  - la delegación de los privilegios de los usuarios entre servicios no es fácil y dificultaría el seguimiento y control de los usuarios.

- **Centrado en el usuario:**

  - En este modelo los usuarios son el centro del diseño, y traslada el control de las identidades de los proveedores de servicio a los propios usuarios, permitiendo a éstos decidir qué identidades necesitan compartir con terceras partes y bajo qué circunstancias.

  - Este modelo encaja perfectamente con la filosofía SSO, la delegación de acceso y la comodidad en el uso de contraseñas por parte de los usuarios.

  - Satisface todos los requerimientos de los usuarios: implementa un ciclo de vida en la gestión de las identidades, y permite protección de identidad y revelación de identidades.

- En [MALIKI2007] se citan una serie de reglas que deben cumplir los sistemas basados en este paradigma:

  - Potenciar el control total de los usuarios sobre su privacidad.
  - Facilidad de uso. Que los usuarios puedan utilizar la misma identidad para cada transacción.
  - Proveer una experiencia de usuario homogénea, con un interfaz de identidad uniforme.
  - Evitar los ataques de suplantación de identidad (por ejemplo *phising*).
  - Limitar la accesibilidad a agentes no autorizados para evitar molestias (como por ejemplo *spam*).
  - Revisar las políticas cuando sea necesario, tanto de los proveedores de identidad como de los proveedores de servicios.
  - Posibilitar la escalabilidad. Basado en que el proveedor de identidad no tiene por qué tener ningún conocimiento previo sobre el proveedor de servicios.
  - Garantizar condiciones de seguridad en el intercambio de datos.
  - La disociación entre la identidad digital y las aplicaciones.
  - Permitir la pluralidad de operadores y tecnologías.

Algunos ejemplos de sistemas basados en este paradigma son: *open-ID*, *Windows Infocard/CardSpace* [JO2009], *Lightweight Identity [JØSANG2005]*, *Simple eXtensible Identity Protocol*[10] (SXIP) o *Higgins*[11].

Como conclusión a este punto de modelos de sistemas de gestión de identidad, señalar que la mayoría de la bibliografía descrita está muy orientada a la gestión de identidades en grandes sistemas, normalmente interconectados por redes de área extensa, ubicados en diferentes países (lo que genera nuevos retos) y con acceso a múltiples servicios como la identificación ante administraciones públicas, comercio electrónico, etc…

[10] *http://www.sxip.com/ (web caída en la comprobación de Enero de 2013)*
[11] *http://www.eclipse.org/higgins/*

2.2. Implementación técnica: Seguridad y confianza en procesos industriales y comerciales

En este apartado se van a revisar las técnicas, métodos y tecnologías orientadas a garantizar la seguridad y confianza en los procesos industriales y comerciales de los que vamos a hacer uso en el desarrollo de esta tesis. Dado que la prueba de concepto del sistema propuesto en esta tesis está relacionada con la trazabilidad, la tecnología RFID y las firmas agregadas, se ha considerado adecuado añadir un apartado con una introducción relativa a estos temas.

Además, se ha añadido un anexo (ver Anexo III) con una revisión sobre criptografía ligera, es decir, sistemas criptográficos que son integrables en etiquetas RFID.

2.2.1. Trazabilidad

2.2.1.1. Trazabilidad General

Según la Real Academia Española de la Lengua, en el avance de su 23ª edición, se define trazabilidad como:

> **1.** *f. Posibilidad de identificar el origen y las diferentes etapas de un proceso de producción y distribución de bienes de consumo.*
>
> **2.** *f. Reflejo documental de estas etapas.*

Esta definición es aplicable a cualquier producto manufacturado o comercializado, siendo usual que coincidan las dos acepciones, es decir, tanto la posibilidad de identificar los diferentes pasos, como el reflejo de dichas etapas, métodos o procesos documentalmente. De hecho, la definición establecida por la norma ISO 9000:2000, recoge ambas acepciones:

> ***"Trazabilidad:*** *capacidad de rastrear la historia, aplicación o localización de todo aquello que esté bajo consideración"*

A pesar de la existencia de definiciones estandarizadas, diversos autores han presentado trabajos relacionados con este concepto, como recoge [CANAVARI2010]. A continuación se citan algunos a modo de ejemplo:

- Taxonomía de los sistemas de trazabilidad [HOBBS2004].
- Definiciones de términos de la identidad de los actores en la cadena de producción [HOBBS2004, POULIOT2008].
- Sobre la identificación por unidades y lotes y la importancia de la documentación entre empresas [SCHIEFER2008].
- Relacionando la preservación de la identidad con la calidad y la seguridad de los alimentos [HOBBS2005].

A la vista de todo lo anterior, en este trabajo nos referiremos a la trazabilidad en general según la definición de la ISO, es decir *capacidad de rastrear la historia, aplicación o localización de todo aquello que esté bajo consideración*.

La trazabilidad en procesos de producción tiene múltiples ventajas que abarcan diferentes ámbitos. Como se indica en [MAI2010], las principales ventajas, descritas en [BUHR2003, CHRYSSOCHOIDIS2009, KARKKAINEN 2003, POGHOSYAN2004, POULIOT2008, SMYTH2002, SPARLING2006, WANG2009] son las siguientes:

- Crecimiento en cuota de mercado e ingresos.
- Posibilidad de poner precios más elevados al poder ofrecer productos "Premium".
- Retiradas de productos menos frecuentes. Se habla de retirada cuando por algún motivo algún producto debe ser retirado del mercado y de la circulación por algún defecto o tipo de problema (por ejemplo, es común la llamada a revisión de algunos automóviles cuando se detecta algún fallo grave para la seguridad, o la retirada del mercado de lotes de alimentos que puedan ser potencialmente peligrosos).
- Reclamaciones y demandas judiciales menos frecuentes y de menor gravedad. En caso de litigio, permite demostrar, si es el caso, la responsabilidad de una infracción.
- Reducción de costes en los seguros de responsabilidad civil.
- Mejora en la gestión de inventarios.
- Reducción de costes por productos caducados o en mal estado (el sistema es capaz de avisar y por tanto se pueden evitar estos problemas con el *stock*).
- Mejora del rendimiento en general de los procesos.
- Ahorro de costes laborales.

- Cumplimiento de normas y legislación de seguridad.
- Mejora la confianza del cliente.
- Posibilidad de solucionar errores en el seguimiento de los productos.
- Mejora la reputación de la empresa de cara a los clientes, proveedores, consumidores y administraciones públicas.
- Permite ser tecnológicamente competente en nuevas tecnologías y procesos industriales.

Estas ventajas son aplicables a cualquier proceso productivo, aunque son especialmente importantes cuando se manejan productos perecederos, que pierdan rápidamente valor con el paso del tiempo o que puedan afectar a la salud humana (como los alimentos o los medicamentos).

Aunque el sistema propuesto en esta tesis es aplicable a cualquier entorno comercial en el que exista un proceso de producción en el que deba verificarse el cumplimiento de determinados parámetros en una serie de puntos de control, el prototipo se ha desarrollado para un tipo de industria específico: la industria alimentaria. Por ello, en el siguiente apartado se profundizará en el concepto de trazabilidad en el ámbito alimentario, así como en la normativa aplicable.

2.2.1.2. Trazabilidad en la industria alimentaria

Debido a su importancia para la salud pública y sobre todo después de algunos episodios de alertas alimentarias a nivel internacional, la trazabilidad aplicada a productos alimentarios, es un tema de estudio especialmente importante dentro de la trazabilidad.

También hay que tener en cuenta que estos sistemas una vez implantados en las cadenas de producción alimentaria, permiten proteger a los consumidores de alimentos contaminados, adulterados o falsificados [DEIMEL2008]. Igualmente, en los últimos tiempos tanto la propia trazabilidad como conceptos relacionados con ella, como la confianza o la transparencia, son cada vez más tenidos en cuenta por los gestores del sector alimentario [DEIMEL2008, FRITZ2007, HANF2007].

Para tener una definición acotada a este entorno, se puede recurrir a la aportada por la ISO en su estándar 8402:1994 y apoyada por una regulación del parlamento europeo 178/2002 [European Parliament2002], sin lugar a dudas la

norma más importante y origen de la reglamentación en Europa, en la que se define trazabilidad como:

> *"la capacidad de rastrear y seguir un alimento, pienso, animal destinado a la producción de alimentos o ingredientes a través de todas las etapas de producción y distribución".*

Esta definición, que encaja perfectamente dentro de la que se había citado en el punto anterior, recoge las particularidades del sector agroalimentario.

Como objeto de trabajos de investigación, se puede señalar que la investigación en trazabilidad alimentaria ha sido muy activa en los últimos años. Se han publicado una gran cantidad de artículos científicos relacionados con esta temática. Algunos muy recientes, como [HEYDER2012b], se han centrado en las inversiones realizadas en sistemas de trazabilidad por parte del sector industrial, llegando a la conclusión de que existe una gran presión externa sobre las empresas para aplicar sistemas de trazabilidad, ya que mejora la imagen de la empresa y esto conlleva a que sean percibidos como útiles por los ejecutivos de este sector productivo. El tema de la trazabilidad en producción de alimentos ha sido abordado desde múltiples perspectivas. A continuación se recogen algunas de estas perspectivas y algunos ejemplos [HEYDER2012a]:

- **Centrado en el consumidor**: La confianza del consumidor en los agentes del sector agroalimentario y en la seguridad alimentaria [DE JONGE2008], la percepción por parte del consumidor de la trazabilidad [GELLYNCK2007], o la predisposición de los consumidores a pagar por las mejoras que aporta la trazabilidad [DICKINSON2005, HOBBS2005a][UBILAVA2009].

- **Centrado en los incentivos que tienen los proveedores en participar en la trazabilidad**: [BANTERLE2008, BUHR2003, BULLOCK2000, GOLAN2004, MALTSBARGER2000].

- **Centrado en el impacto de los cambios normativos en los proveedores**: [ARIENZO2008, COFF2008, FLYNN2003].

- **Centrados en implementaciones técnicas**: en el apartado 2.2.2 (tecnología RFID) se citarán unos cuantos trabajos de trazabilidad basados en este tipo de tecnología.

- **Centrados en la inversión y los costes de operación**: [BANTERLE2008, GELLYNCK2007, RESENDE-FILHO2007, THEUVSEN2005].

Por ser un tema relacionado con la salud, existe abundante legislación que regula la trazabilidad en este sector, y que además para muchas industrias y productos es de obligado cumplimiento. Por todo ello, se ha decidido incluir parte de la normativa en el apartado 4.1.1. Además, muchas de las normas fijan la responsabilidad del agente productivo en el caso de problemas de salud relacionados con los alimentos, y por tanto puede ser muy interesante tener un sistema de responsabilidad de los controles, para poder esclarecer quién ha podido realizar mal su tarea en el puesto de control (independientemente por supuesto, de a quién corresponda la responsabilidad última desde el punto de vista jurídico, cuestión ésta que escapa totalmente al ámbito y enfoque de la presente tesis).

2.2.2. Identificación por radiofrecuencia (RFID)

El sistema de identificación por radio frecuencia (RFID) tuvo su origen en la II Guerra Mundial y posteriormente Harry Stockman introdujo el concepto de RFID pasivo [STOCKMAN1948].

Desde entonces, la posibilidad de identificar unitariamente objetos incluso aunque no haya visión directa entre el lector y la etiqueta ha hecho, junto con la posibilidad de guardar información en la propia etiqueta y un coste contenido, que este sistema se esté popularizando, desplazando paulatinamente a otros sistemas de identificación más extendidos, como la identificación mediante código de barras.

La base del sistema es permitir la identificación de objetos o personas mediante un único identificador, el cual se transfiere con un determinado protocolo hasta un dispositivo receptor, denominado lector, mediante ondas de radio [LANDT2005]. Normalmente, el lector se encuentra conectado a un sistema informático, y mediante una aplicación informática se procesan los datos del lector y se relacionan con el sistema de información de la empresa [MCFARLANE2003]. Durante los últimos años esta tecnología ha ido penetrando en diversas industrias, siendo múltiples sus aplicaciones. Por citar algunas, se puede destacar la utilización de etiquetas de proximidad para abrir puertas, inmovilizadores para automóviles, identificación de animales, control de

stocks, pago en peajes, localización de personas (ancianos o niños), sistemas anti-falsificación, etc. En [BANKS2007] y en [ILIE-ZUDOR2011] se pueden encontrar descritas multitud de aplicaciones.

Una de sus aplicaciones más prometedoras para la industria es la que se relaciona con la logística, al poder realizar el seguimiento de un objeto concreto. Los sistemas más extendidos para la identificación de objetos son los códigos de barras, que principalmente estaban definidos por dos estándares: el European *Number Article* (EAN) en Europa y otro de propósito similar en Estados Unidos, el Universal *Product Code* (UPC). Estos dos estándares actualmente se han fusionado en uno único, conocido como GS1 [GS12012]. Aunque en la actualidad ya se han realizado multitud de implementaciones de sistemas de trazabilidad, principalmente mediante códigos de barras, cada vez son más las empresas que complementan este sistema de identificación mediante radiofrecuencia. La tecnología RFID aporta una serie de ventajas principales [SAHIN2002 y WYLD2006]:

- Reducción en los costes de mano de obra.
- Mayor velocidad en la cadena de producción.
- Reducción en las pérdidas (fraudes, robos y errores administrativos).
- Control de productos más eficiente.
- Aumento del conocimiento del comportamiento del cliente.

Específicamente en el sector de la alimentación también tiene tres ventajas muy importantes:

- Mejor gestión de los productos perecederos.
- Mejora en el seguimiento, localización y solución de problemas de calidad de los productos.
- Mejora de la gestión de retirada de productos cuando existan riesgos con alguno de ellos.

En este sector, donde los sistemas de trazabilidad son obligatorios, la falsificación no es un hecho nuevo. En una revisión histórica de este fenómeno [SHEARS2010], la falsificación en productos alimentarios, se documentan falsificaciones desde civilizaciones tan antiguas como la griega o la romana [SUMAR1995] hasta nuestros días. También señalar que paralelamente, y para contrarrestar estas amenazas, se han ido desarrollando complejos procedimientos científicos para detectar los fraudes alimentarios, como por ejemplo las huellas de

ADN [HUANG2011], la identificación de determinados compuestos [TEDESCHI2011] y otros tipos de análisis [ALAÑÓN2011].

En esta línea, y a modo de ejemplo, cabe señalar que en los primeros meses de 2013, con este tipo de técnicas se detectó un fraude relativo a la composición de hamburguesas, que se anunciaban como 100 % vacuno y contenían porcentajes importantes de carne de caballo. También gracias a la trazabilidad, las empresas que distribuían estas hamburguesas pudieron saber perfectamente los proveedores que les habían suministrado la carne y las plantas de producción donde fueron elaboradas, lo que ayudó en gran medida a esclarecer responsabilidades.

Aunque la trazabilidad facilita la gestión de la producción, la distribución y la logística, no garantiza que los productos no sean falsificados. Sin embargo, realizando la trazabilidad sobre tecnología RFID podemos poner más trabas a las falsificaciones. Aunque no es su objetivo principal, el sistema propuesto en esta tesis también contribuye en la tarea de dificultar la falsificación de productos, haciendo que sean fácilmente detectables las etiquetas falsas (no tienen una firma válida asociada a su identidad digital) o clonadas (no corresponden los atributos de la identidad digital con los del producto). Por tanto, se puede afirmar que una trazabilidad segura es vital para ayudar a prevenir y detectar los fraudes.

En el párrafo anterior se ha hablado de trazabilidad segura, pero realmente, ¿qué es trazabilidad segura? Según [FAYOLLE2008] "la trazabilidad segura es la posibilidad de rastrear las líneas de productos que una compañía lanza al mercado, previniendo los ataques al propio sistema de rastreo". Una forma de conseguir esto, es incorporar a los datos de la trazabilidad las características específicas e individuales de cada producto, de manera que permita ser identificado inequívocamente, lo que se denomina deflectometría [FAYOLLE2008]. Esta técnica, similar a la identificación biométrica usada con seres humanos, es difícil de aplicar en cadenas de producción y especialmente en productos que varían su estructura y fisiología con el tiempo.

Otra posibilidad de trazabilidad segura, es incorporar al sistema de trazabilidad los atributos relevantes del producto, que conformarán su identidad digital, y que serán proporcionados por operarios, compañías, individuos o máquinas que lleven a cabo las verificaciones de las características de calidad esenciales, tras las diversas etapas de producción.

Aunque existen métodos para garantizar los datos que acompañan al producto, como por ejemplo la creación de un círculo de confianza (CoT, *Circle of*

Trust) [BOURSAS2008] en las diferentes partes de la cadena de suministro [HE2008], en el presente trabajo se propone otra alternativa: la identificación de los agentes involucrados en el proceso de trazabilidad y verificación de la calidad mediante el uso de una única firma electrónica por producto, que permita identificar qué agentes han realizado los controles y han introducido la información en el sistema. Esto permite dotar al producto de una identidad digital propia, grabada en la etiqueta RFID y avalada por un conjunto de entidades que a su vez poseen su propia identidad digital. Además, también es necesario introducir marcadores de confianza, para así a su vez incrementar la confianza de los consumidores [LEE2007].

2.2.2.1. Hardware

La expresión más sencilla de un sistema de identificación por RFID, como se muestra en la Fig. 2-5, consta de un dispositivo identificador (normalmente denominado transpondedor RFID, o simplemente etiqueta RFID o *tag*) que se une al objeto o ente a identificar, un lector RFID o transceptor capaz de leer y/o escribir las etiquetas y un protocolo que define el formato de la información y el procedimiento de lectura/escritura.

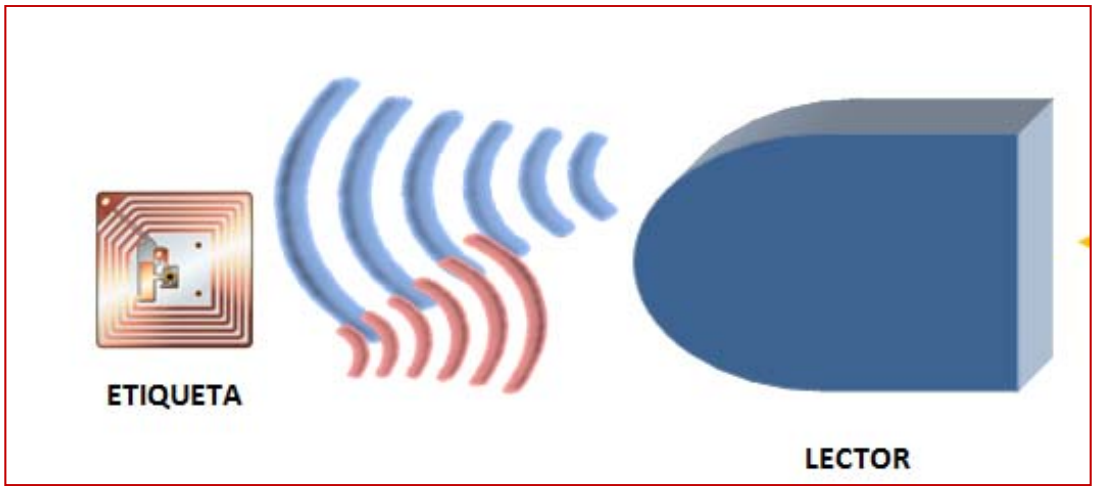

Fig. 2-5. Esquema básico de un sistema RFID.

Como se señala en [WYLD2006], los elementos básicos que conforman una etiqueta RFID son tres: el chip con capacidades de cálculo y memoria muy limitadas, un elemento de acoplo electromagnético (antena) y el encapsulado.

Respecto al lector, que en realidad es un lector grabador, consta de un módulo de radiofrecuencia, una unidad de control, y un elemento de acoplo electromagnético con el que interrogar a las etiquetas por medio de radiofrecuencia. Dada la reducida capacidad de cálculo y de almacenamiento del lector, en muchos casos también se utiliza un sistema computacional de apoyo, como se muestra en la Fig. 2-6.

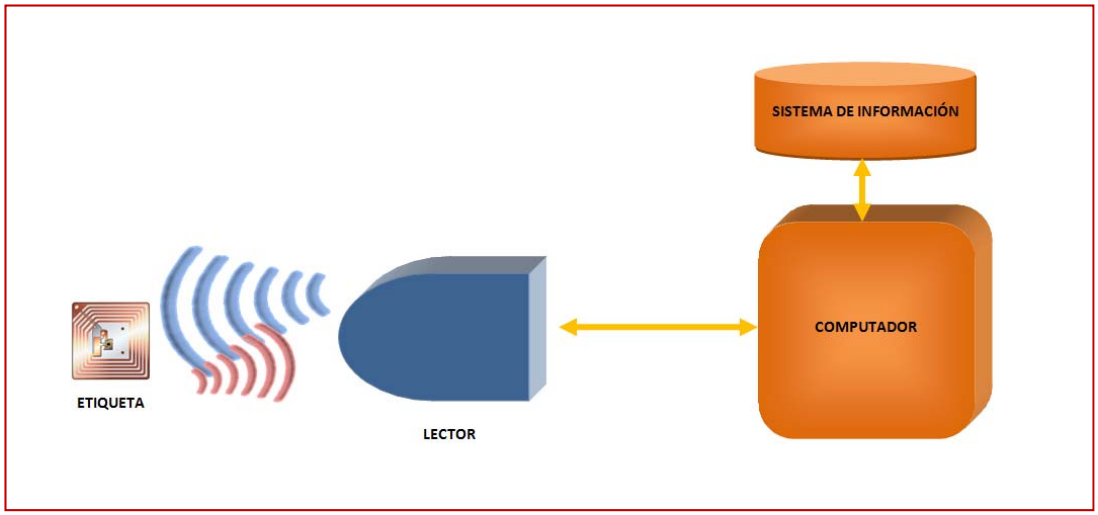

Fig. 2-6. Esquema extendido de un sistema RFID.

Los sistemas RFID se basan en una comunicación inalámbrica bidireccional entre los lectores/grabadores y las etiquetas por medio de ondas de radiofrecuencia (utilizando diferentes bandas de transmisión, comprendidas entre 125 KHz y 2.4 GHz).

Dado que para trazabilidad las etiquetas más utilizadas son las pasivas, debido a su bajo coste, a continuación se van a describir brevemente los métodos de comunicación entre los lectores y las etiquetas pasivas. Esta comunicación se basa en la transmisión simultánea de energía y datos [GLOVER2006], utilizando las etiquetas la componente magnética, la eléctrica o ambas de la señal electromagnética que genera el lector, para obtener energía para funcionar y enviar su respuesta. Normalmente esta transferencia de energía se realiza mediante acoplamiento. El tipo de acoplamiento determina la manera en la que se produce la transmisión de energía y datos entre el lector y la etiqueta. Los principales tipos de acoplamiento utilizados en las comunicaciones con transpondedores pasivos son [PERIS-LOPEZ2008]:

- ***Backscatter* Pasivo**: El lector genera durante un tiempo una onda de radiofrecuencia, cuando un transpondedor entra en el área de influencia de la señal, la demodula en un patrón binario, que contiene una serie de

comandos predeterminados que le indican a la etiqueta la operación a realizar. La etiqueta obtiene la energía del campo electromagnético generado por el lector al realizar la comunicación con el transpondedor. Para contestar, el transpondedor modula la señal que está enviando el lector, de modo que le llegue reflejada pero conteniendo la información que le envía la etiqueta. Para ello el transpondedor varía la impedancia de su antena (sintonizando y desintonizando), mediante la variación del valor de la resistencia de carga, lo que permite enviar una señal binaria codificada como respuesta al lector. Una representación muy básica de este concepto se representa en la Fig. 2-7.

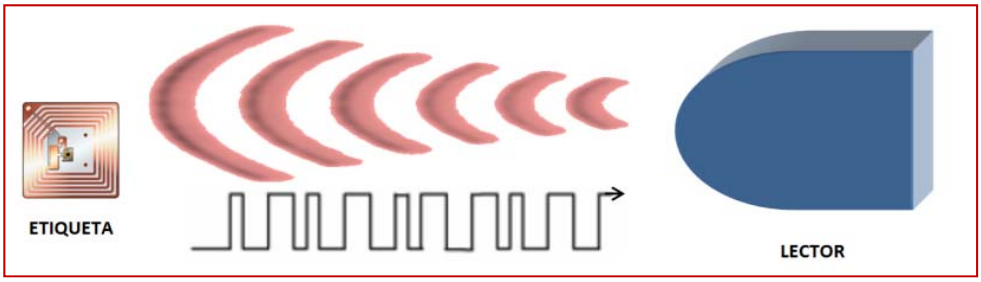

Fig. 2-7. Acoplamiento *Backscatter* pasivo

- **Acoplamiento inductivo (magnético):** Cuando un conductor es afectado por un campo magnético, se induce en él una corriente eléctrica. Este fenómeno físico es conocido como acoplamiento inductivo, ya que la corriente es inducida por la exposición a un campo magnético. Este tipo de acoplamiento suele utilizarse en sistemas LF (baja frecuencia) o HF (alta frecuencia), y por las propias características del campo magnético sólo puede utilizarse a poca distancia del emisor, aunque este aspecto puede ser utilizado algunas veces como medida de seguridad (un atacante deberá estar muy cerca de una etiqueta para poder interactuar con ella). La antena del lector es excitada con una corriente eléctrica para generar un campo magnético, que a su vez inducirá una corriente en la antena del transpondedor cuando penetre en dicho campo magnético, y que será la que permita alimentar a los componentes electrónicos de la etiqueta. En la Fig. 2-8 se muestra una esquematización de este sistema, incluyendo dos componentes inductivos tanto en el emisor como en el receptor. Para

responder, la etiqueta variará la impedancia de carga de la antena en función de los datos binarios a transmitir, lo que provocará una modulación en el campo magnético generado por el lector. La información transportada mediante esta modulación, será obtenida por el lector mediante la demodulación de la señal.

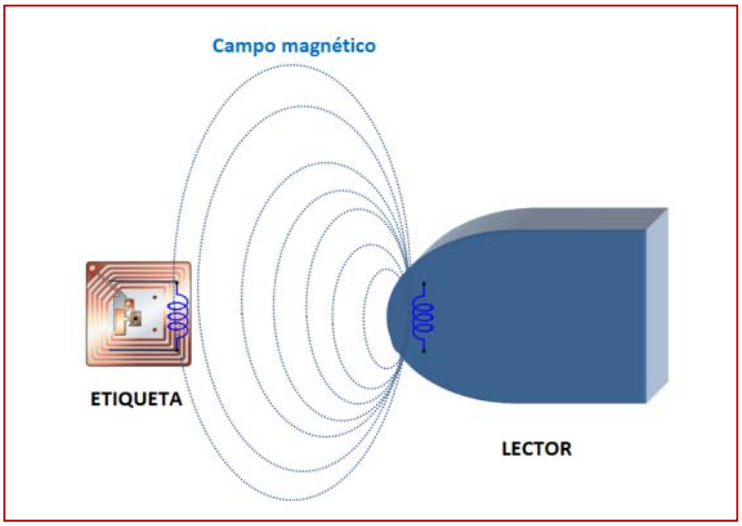

Fig. 2-8. Acoplamiento inductivo (magnético)

- **Acoplamiento electromagnético:** en el acoplamiento electromagnético se utilizan los dos tipos de energía la del campo eléctrico y la del campo magnético. Suele utilizarse en sistemas de UHF (frecuencia ultra alta) y microondas. Cuando están cerca del lector utilizan el campo magnético para obtener la energía (si han sido diseñadas con esta capacidad), y cuando se encuentran a distancias mayores utilizan el campo eléctrico para hacer resonar la antena de la etiqueta a una determinada frecuencia normalmente utilizando la técnica de acoplamiento *backscatter* referida anteriormente.

Además del acoplamiento, otros factores claves en la comunicación entre los lectores y las etiquetas pasivas son [PERIS-LOPEZ2008]:

- **Codificación de datos:** para una codificación de datos eficiente, se utilizan técnicas de modulación y codificación. Es importante tener en cuenta que los lectores no tienen restricciones importantes de energía para transmitir, pero sí las tienen en el ancho de banda. Por el contrario las

etiquetas pasivas tienen una limitación importante en la energía. Atendiendo a esta circunstancia, suele utilizarse en la comunicación lector-etiqueta codificación Manchester o NRZ (No Retorno a Cero), mientras que en la comunicación etiqueta-lector suelen utilizarse codificaciones PPM (Modulación Pulso Pausa), o PWM (Modulación por Ancho de Pulsos).

- **Modulación:** la elección dependerá de los requerimientos de cada caso. Las posibles modulaciones a utilizar son ASK (modulación por desplazamiento de amplitud), FSK (modulación por desplazamiento de frecuencia) y PSK (modulación por desplazamiento de fase).

- **Protocolos anticolisión:** son los encargados de posibilitar la atención de varias peticiones simultáneas. Se pueden implementar tanto en las etiquetas como en los lectores.

    - **de etiquetas:** son los encargados de posibilitar que varias etiquetas contesten a la consulta de un lector de forma simultánea. Suelen estar basados en los protocolos de acceso al medio en canales de difusión de las redes de ordenadores, pero teniendo en cuenta las limitaciones de los sistemas RFID. Normalmente combinan soluciones probabilísticas y determinísticas. Para mayor información se recomienda la lectura de [Lei Zhu2011].
    - **de lectores:** son necesarios cuando varios lectores interrogan de forma simultánea a una etiqueta. Las soluciones suelen basarse en la utilización de varias frecuencias a lo largo del tiempo. En [JOSHI2008] se presentan diversos protocolos.

En esta breve introducción se han presentado los conceptos básicos de funcionamiento de los sistemas RFID. Si se desea ampliar la información sobre el proceso físico de la comunicación con las etiquetas se recomienda la lectura de [WANT2006] y [BANKS2007]. A continuación, se va a profundizar un poco más en las etiquetas utilizadas, ya que van a suponer el volumen de inversión más importante dentro del sistema, y por tanto su correcta elección es fundamental.

En los sistemas RFID, en función de la aplicación y el entorno de trabajo se deberá utilizar un tipo u otro de etiqueta. Los principales parámetros que afectan

al comportamiento de una etiqueta y por tanto su adecuación a un entorno concreto son: absorción, reflexión, efectos dieléctricos y efectos de propagaciones complejas. En sistemas reales, el coste de explotación más importante del sistema es el relativo a la adquisición de las etiquetas, ya que deben encargarse en volúmenes muy elevados y por tanto el precio unitario es fundamental, ya que debe multiplicarse por valores muy grandes. También para seleccionar la etiqueta se debe tener en cuenta el tipo y tamaño del objeto a identificar, así como las condiciones ambientales del entorno de trabajo. Como ejemplo, se puede señalar que los objetos a identificar pueden ir desde un animal vivo [VOULODIMOS2010] hasta pequeñas bolitas de mineral de hierro [KVARNSTRÖM2010]. El núcleo de la etiqueta es un circuito integrado que almacena tanto el número de identificación único como otros datos, si tiene un área de memoria disponible para tal efecto. Este circuito va unido a una antena, y finalmente va todo recubierto y protegido por un encapsulado. En función de las condiciones de trabajo, se seleccionará el encapsulado más apropiado para proteger el interior de factores ambientales que puedan deteriorarlo, como pueden ser: el polvo, temperaturas extremas, humedad, calor, sal,... Por ello, es importante a la hora de elegir el tipo de etiqueta seleccionar un encapsulado que soporte las condiciones de la cadena de producción.

Una clasificación inicial muy sencilla sería distinguir las etiquetas según su tipo de memoria, entre etiquetas grabables (en inglés *writable*) y etiquetas de sólo lectura o no grabables (en inglés *non-writable)*. Las etiquetas pueden ser totalmente regrabables (permite modificar la memoria tantas veces como se desee), grabable una sola vez o de sólo lectura. Dependiendo del tipo de etiqueta, la introducción de información, es decir la escritura (grabado) de la etiqueta, será en el proceso de fabricación o a nivel de aplicación.

Si bien es cierto que la clasificación anterior es utilizada en algunas ocasiones, es poco exhaustiva por lo que en general se suele recurrir a otras clasificaciones, como la utilizada en [BARJIS2010] y que clasifica las etiquetas según: si poseen batería o no (se denominan activas o pasivas), su frecuencia de trabajo, su capacidad de almacenamiento de datos, su adecuación a usos determinados *("capability")*, tiempo de vida operativo y coste. Teniendo en cuenta estos parámetros, junto con los requerimientos de encapsulado, es posible seleccionar el transpondedor más adecuado para cada necesidad.

Según el estándar EPCGlobal citado en [GARFINKEL2005], las etiquetas se pueden clasificar en seis clases:

- Clase 0: son pasivas (obtienen la energía de la señal enviada por el lector), sólo permiten su lectura y la información es escrita en la etiqueta por el fabricante de la etiqueta. Dentro de este tipo se encuentra las etiquetas antirrobo o EAS (Electronic Article Surveillance).

- Clase 1: son pasivas, permiten su escritura una única vez. Normalmente se les graba un código identificador único como el EPC (Electronic Product Code).

- Clase 2: son pasivas o semipasivas (incluyen una pequeña batería pero sólo transmiten a petición del lector), muy similares a las de clase 1 pero permiten múltiples escrituras.

- Clase 3: semipasivas, similares a las de clase 2 pero incluyen sensores.

- Clase 4: son activas, integran baterías y transmisores por lo que pueden comunicarse directamente con otras etiquetas además de con el lector.

- Clase 5: son activas, similares a las de clase 4, pero añaden la posibilidad de comunicarse con otras etiquetas y/o dispositivos.

Las etiquetas activas, que tienen una fuente propia de energía, permiten mayores distancias de trabajo y mayor velocidad que las pasivas, siendo su principal problema que son de mucho mayor tamaño y notablemente más caras. Por el contrario, las pasivas pueden integrarse en pequeñas etiquetas adhesivas, hojas de papel o incluso en encapsulados del tamaño de un grano de arroz. En la Tabla 2-3, basada en [WYLD2006] se comparan las características de ambos tipos de etiquetas. El tiempo de vida suele ser mucho más corto en las etiquetas activas, ya que cuando se gasta la batería dejan de funcionar.

Otro parámetro fundamental es la banda de frecuencia de trabajo. El uso de una u otra banda condicionará la distancia a la que puede funcionar el lector y la tarjeta, así como la posibilidad o no de leer varias etiquetas al mismo tiempo. Las bandas típicas de trabajo de estos sistemas son las bandas de LF (125-134.2 KHz), HF (13.56 MHz), UHF (865.5-867.6 MHz en Europa, 915 MHz en Estados Unidos y 950-956 MHz en Japón) e ISM (2.4 GHz). Las dos primeras bandas suelen utilizarse para identificación de animales y sistemas de entrada "sin clave", la tercera se emplea masivamente para etiquetas inteligentes e identificación de objetos con fines logísticos y la cuarta también para identificación de objetos. Recordar que cuanto mayor es la frecuencia, mayor es la tasa de transmisión de datos, pero aparecen más problemas para transmitir en

zonas de alta humedad, superficies mojadas o con gran cantidad de superficies metálicas.

Etiqueta Pasiva	Etiqueta Activa
• No tiene batería para alimentarse	• Se alimenta de una batería interna
• Más económica	• Más cara
• Mayor duración (no depende de la batería)	• Duración hasta que se agota la batería
• Más ligera	• Más pesada (sobre todo por la batería)
• Menos rango (3 a 5 metros)	• Mayor rango (hasta 100 m)
• Afectada por el ruido electromagnético	• Mejor inmunidad al ruido
• Obtiene la energía del campo electromagnético generado por el lector	• Obtiene la energía de la batería que posee para transmitir al lector
• Requiere lectores potentes	• Puede funcionar con lectores menos potentes
• Menor velocidad de transmisión de datos	• Mayor velocidad de transmisión de datos
• Menos etiquetas pueden ser leídas de forma simultánea	• Más etiquetas pueden ser leídas de forma simultánea
• Gran sensibilidad a la orientación	• Menos sensibilidad a la orientación

Tabla 2-3. Comparación entre etiquetas pasivas y activas.

El contenido de la etiqueta es básicamente un número identificador único. Adicionalmente suele llevar una memoria en la que se pueden grabar datos, y en las etiquetas securizadas se presenta también una zona de memoria cifrada, para cuya utilización es necesario conocer una clave secreta.

A la vista de todo lo anterior, se puede deducir que la arquitectura de una de estas etiquetas consta de: memorias, un sistema de transmisión y recepción con su correspondiente antena y la lógica necesaria para gestionar las tareas de lectura/escritura y cifrado (si posee esta característica).

En cuanto a la capacidad de almacenamiento de datos existen desde 1 bit, usadas en sencillos sistemas antirrobo [GLOVER2006], hasta más de 4 MB. Las actuales velocidades de transferencia están en torno a los 4 Mbps [PILLIN2008],

aunque existen trabajos han propuesto transceptores RFID de banda ultra-ancha que permiten velocidades máximas de hasta 112 Mbps [PELISSIER2011].

Finalmente indicar que el coste de las etiquetas activas ha ido decreciendo (ya está por debajo de los 30 centavos de Dólar estadounidense por unidad), pero son mucho más económicas y aptas para las cadenas de producción las pasivas como señala [VÉRONNEAU2009].

2.2.2.2. Revisión de los aspectos de seguridad en RFID

Aunque en su origen se presentó la tecnología RFID como segura en sí misma, esta creencia fue (y es) uno de sus mayores peligros, ya que si bien ofrece niveles de seguridad mucho mayores que otras tecnologías de identificación, no está exenta de riesgos, aunque en función de la aplicación concreta, el nivel de seguridad requerido y el presupuesto disponible se pueden alcanzar cotas de seguridad perfectamente adecuadas para cada caso.

Existe abundante bibliografía relativa a las amenazas más importantes a las que debe enfrentarse la tecnología RFID. Muchos de los trabajos existentes se centran en las amenazas relacionadas con la privacidad [AVOINE2005, AYOADE2007, GARFINKEL2005]. En [KARYGICMNIS2006] se propone una taxonomía que añade tres nuevos grupos de riesgos al ya mencionado de la privacidad: riesgos de "procesos de negocios" *(business process risks)*, relacionados con el impacto de fallos del sistema de RFID en sistemas automáticos basados en él; riesgos de "inteligencia de negocios" *(business intelligence risks)*; y riesgos "externos". Aunque esta perspectiva es más extensa y cercana a la realidad que las primeras, ya que abarca más tipos de amenazas, parece especialmente interesante y completa la clasificación propuesta en [MITROKOTSA2010, MITROKOTSA2009], donde se agrupan los tipos de ataques y amenazas relacionándolos con un modelo de cuatro capas: física, red y transporte, aplicación y estratégica. Las tres primeras se corresponden bastante bien con las capas correspondientes del modelo OSI de redes de computadores, la cuarta engloba los riesgos relacionados con factores logísticos y además también se plantea la posibilidad de que los ataques sean multicapa, es decir, afecten a varias de las capas básicas.

Como se desarrolla en [MITROKOTSA2010, MITROKOTSA2009], los principales riesgos de cada capa son:

- **Capa física**:
  - Inhibición permanente de las etiquetas: abarca todos los procedimientos cuya finalidad es impedir la comunicación de la tarjeta permanentemente (utilización de comandos específicos, dañando la etiqueta, quitándola del objeto,…).
  - Inhibición temporal de las etiquetas: igual que el anterior pero sólo temporalmente (jaulas de Faraday, interferencias,…).
  - Inhibición o eliminación de los lectores: consiste en atacar físicamente los lectores.
  - Ataques de repetición: consiste en enviar al lector RFID una copia de una señal emitida por una etiqueta válida. Se consigue escuchando la transmisión de la original.

- **Capa de red y transporte:**
  - Suplantación de la identidad (afectan a las tarjetas): consiste en la transmisión de información falsa, por parte de la etiqueta, que el lector procesa como válida. Por ejemplo, se podría enviar un código electrónico de producto (EPC) falso, de un producto para que el sistema de pago lo procese como uno mucho más económico.
  - Suplantación y escuchas no autorizadas (afectan a los lectores): un lector se hace pasar por otro para poder acceder a la información de una etiqueta y obtiene los datos, o directamente un atacante obtiene la información del canal de comunicación.

- **Capa de aplicación:**
  - Lecturas no autorizadas de las etiquetas.
  - Modificación de las etiquetas: el objetivo es modificar la información contenida en la etiqueta
  - Ataques relacionados con el middleware: como desbordamiento de buffers e inyección maliciosa de código.

- **Capa estratégica:**
  - Espionaje industrial.
  - Técnicas de ingeniería social.
  - Amenazas a la privacidad.
  - Selección de objetivos: por ejemplo detectar personas con artículos de lujo para atracarlos.

- **Amenazas multicapa:**
  - Ataques de denegación de servicio.
  - Lectura / escritura de información en el espacio libre de la tarjeta sin conocimiento del usuario.
  - Análisis de tráfico: con el fin de extraer información de la etiqueta estudiando las comunicaciones (cuantos más mensajes se capturen, mayor efectividad tendrá el ataque por análisis de tráfico).Ataques a los algoritmos de cifrado de la información.
  - Ataques basados en la monitorización de parámetros físicos de funcionamiento: consumo de energía, variación en los campos electromagnéticos, etc…
  - Ataques de repetición: grabar una contraseña de una transacción anterior y repetirla cuando se presente el mismo desafío.

En el apartado 4.5, se profundiza más en los tipos de ataque y cómo abordar su protección.

2.2.3. Firmas agregadas.

La seguridad del sistema propuesto se basa en el uso de un concepto criptográfico denominado firma agregada, estrechamente relacionado con la idea de multifirma. En este apartado se va a realizar una breve revisión de los aspectos básicos relacionados con esta herramienta.

El concepto criptográfico de multifirma, se basa en que N agentes firmen un mismo mensaje, de manera que un verificador pueda comprobar que todos ellos han firmado el mensaje. Esta idea fue propuesta por primera vez por Itakura y Nakamura [ITAKURA1983], y después ha sido objeto de múltiples trabajos de investigación como por ejemplo [BOLDYREVA2002, OKAMOTO1988]. La primera propuesta de una multifirma, en la cual las firmas individuales eran convertidas directamente en una multifirma fue realizada por Boldyreva en [BOLDYREVA2002], que además conseguía notables mejoras sobre los sistemas de firma electrónica tradicionales, como un tamaño de firma mucho menor a la concatenación de todas las firmas aplicadas, y una importante reducción del tiempo de cómputo invertido en realizar la verificación. A su vez, el esquema de Boldyreva estaba basado en firmas BLS [BONEH2004].

Las firmas agregadas van un poco más lejos que las multifirmas, ya que permiten compactar todas las firmas implicadas en la multifirma, en una única firma

agregada, que puede ser verificada conociendo únicamente las claves públicas de los firmantes y los diferentes mensajes. Notar que ahora en lugar de un mensaje único como en el caso de la multifirma, se debe incorporar un mensaje diferente por cada firmante.

Existen diversas implementaciones de esta idea, como las firmas agregadas en paralelo [BONEH2003], también conocido como esquema BGLS, en el que la verificación es independiente del orden de firma. Otra implementación destacada la constituyen las firmas agregadas secuenciales [LYSYANSKAYA2004], que permiten verificar tanto la validez de la firma como el orden en el que se firmaron los mensajes. Posteriormente, se propusieron las firmas agregadas basadas en la identidad [HERRANZ2006], que permiten realizar el proceso de firma sin necesidad de certificados (a costa de requerir una entidad confiable maestra).

Como ya se ha mencionado, el tamaño de memoria disponible para grabar las firmas es un recurso muy limitado en el entorno de trabajo en el que se centra esta tesis, por lo que una propiedad muy importante que debe poseer el método que se utilice es que la firma agregada sea de un tamaño constante e independiente del número de firmas que se compacten. Teniendo en cuenta lo anterior, se ha seleccionado la propuesta de Boneh [BONEH2003] que basada en el uso de aplicaciones bilineales cumple el requisito anteriormente descrito. Así pues, y tal como lo exponen los propios autores en [BONEH2001], se puede definir la firma agregada de la siguiente manera:

"Considérese un conjunto $\mathbb{U}$ de usuarios, donde cada usuario $u \in \mathbb{U}$, posee una pareja de claves de firma, una privada y otra pública (PK_u y SK_{u-}). Se desea agregar las firmas de un subconjunto $U \subseteq \mathbb{U}$. Cada usuario $u \in U$, produce una firma σ_u de un mensaje M_u, generado por él. Estas firmas son combinadas en una firma agregada σ por una tercera parte no confiable, que se denominará "agregador". Para poder verificar las firmas, es suficiente con tener acceso a las claves públicas de los usuarios, a los mensajes y a las firmas de los mensajes, pero no es necesario conocer ninguna clave privada. El resultado de esta agregación es una firma agregada σ del mismo tamaño que cualquiera de las firmas individuales. Esta firma agregada σ tiene la propiedad de que, dada al verificador junto con las identidades de las partes implicadas y con los mensajes, puede considerarse una prueba de que cada usuario ha firmado su respectivo mensaje."

Esta agregación se basa en el esquema co-Gap Diffie Hellman (co-GDH). Para presentar los conceptos relacionados con este esquema, se va a utilizar la siguiente notación:

1. G_1 y G_2 son dos grupos cíclicos con el mismo orden primo p;
2. g_1 es un generador de G_1 y g_2 es un generador de G_2.
3. ψ es un isomorfismo computable desde G_2 hasta G_1, con $\psi(g_2) = g_1$;
4. e es una aplicación bilineal computable e: G_1 x $G_2 \rightarrow G_T$.

En primer lugar vamos a introducir los problemas Diffie-Hellman Computacional (CDH) y Diffie-Hellman Decisional (DDH). Con la notación anterior, tomando $G_1=G_2=G$, siendo G un grupo cíclico multiplicativo de orden primo con generador g, podemos definir los siguientes problemas:

- ***Diffie-Hellman computacional***: dados $g, g^a, h \in G$ computar $h^a \in G$.
- ***Diffie-Hellman decisional:*** dados $g, g^a, h, h^b \in G$ generar el resultado "SI" en el caso de que $a=b$, y "NO" en cualquier otro caso. Las tuplas de esta forma – (g, g^a, h, h^b)– son denominadas tuplas Diffie-Hellman.

Para manejar el caso $G_1 \neq G_2$ Boneh, Gentry, Lynn y Shacham definieron los problemas co-CDH y co-DDH [BONEH2001]. Cuando $G_1 = G_2$, estos problemas se reducen a los problemas estándar CDH y DDH, que acabamos de exponer. Con estas consideraciones, se obtienen las siguientes generalizaciones naturales de los problemas CDH y DDH:

- ***Co-Diffie-Hellman computacional***: dados $g_2, g_2^a \in G_2$ y $h \in G_1$ computar $h^a \in G_1$.
- ***Co-Diffie-Hellman decisional:*** dados $g_2, g_2^a \in G_2$ y $h, h^b \in G_1$ generar el resultado "SI" en el caso de que $a=b$, y "NO" en cualquier otro caso. Cuando el resultado es "SI" se puede afirmar que (g_2, g_2^a, h, h^a) es una tupla co-Diffie-Hellman.

A continuación trabajaremos con grupos co-GDH que serán parejas de grupos G_1 y G_2, en las cuales co-DDH es sencillo computacionalmente pero co-CDH es muy complejo. Esta facilidad para el co-DDH la conseguimos mediante la utilización de emparejamientos bilineales.

Los emparejamientos bilineales surgieron como métodos de criptoanálisis de sistemas criptográficos basados en curvas elípticas, reduciendo el problema de cálculo del logaritmo elíptico en curvas supersingulares al del logaritmo discreto, más fácilmente computable [MENEZES1993]. Luego el ataque fue extendido incluyendo otros tipos de curvas más generales [FREY1999,

GAREFALAKIS2004]. Señalar que existe abundante bibliografía sobre los algoritmos que permiten implementar emparejamientos bilineales basados en los emparejados de Weil y Tate, normalmente apoyados en los trabajos de Miller [MILLER2005].

En nuestra implementación n=|G_1|=|G_2|=|G_T|. Un emparejamiento bilineal es una función e: G_1 x G_2 → G_T con las siguientes propiedades:

1. Bilineal: para todo $u \in G_1, v \in G_2$ y $a, b \in \mathbb{Z}$, $e(u^a, v^b) = e(u, v)^{ab}$.
2. No degenerativo: $e(g_1, g_2) \neq 1$.

Estas propiedades implican dos más:

- Para cualquier $u_1, u_2 \in G_1, v \in G_2, e(u_1 u_2, v) = e(u_1, v) \cdot e(u_2, v)$.
- Para cualquier $u, v \in G_2$, $e(\psi(u), v) = e(\psi(v), u)$.

En definitiva, un emparejamiento bilineal es una función que proyecta dos elementos de los grupos G_1 y G_2, sobre un elemento del grupo G_T:

$$e: G_1 x\, G_2 \rightarrow G_T$$

donde G_1 y G_2 son subgrupos del grupo de puntos de una curva elíptica, dependiendo del emparejamiento que tomemos (Weil o Tate) y G_T es el grupo multiplicativo $\mathbb{Z}_n$.

Una vez presentado el concepto de emparejamiento bilineal, a continuación se va a mostrar un esquema de firma basado en el esquema presentado en [BONEH2001]. Este comprende tres algoritmos: generación de clave (*keygen)*, firma (*sign*) y verificación (*verify)*, y usa una función *hash*[12] de dominio completo H:{0,1}* → G_1. Esta función *hash map-to-point* asigna a una cadena de longitud arbitraria, un punto de una curva elíptica definida sobre un cuerpo finito.

- **Generación de clave:** tomar un número aleatorio $x \overset{R}{\leftarrow} \mathbb{Z}_n$, y computar $Q \leftarrow xP$. La clave pública será $Q \in G_2$, la clave secreta será $x \in \mathbb{Z}_n$ y $P \in G_2$ será un parámetro público del sistema.

[12] *Aunque habitualmente en la traducción del término hash al español, suelen utilizarse términos como función picadillo o función resumen, el autor considera que el término original en inglés está suficientemente extendido para comprenderse perfectamente en su expresión original en lengua inglesa.*

- **Firma:** dada una clave secreta x y un mensaje $M \in \{0,1\}^*$, computar $R \leftarrow H(M)$, donde $R \in G_1$ y $\sigma \leftarrow xR$. La firma será $\sigma \in G_1$.
- **Verificación:** dada una clave pública Q, un mensaje M, y una firma σ, computar $R \leftarrow H(M)$ y verificar que (P, Q, R, σ) es una tupla co-Diffie-Hellman válida, es decir $e(R, Q) = e(\sigma, P)$.

Una vez introducido el concepto de firma agregada y de emparejamiento bilineal, se puede retomar el concepto de firma agregada, concretamente el esquema basado en firmas co-GDH, que es el que se ha utilizado en esta tesis, comúnmente conocido como firma agregada BGLS, en honor a sus autores: Dan Boneh, Craig Gentry, Ben Lynn y Hovav Shacham.

Como ya se ha comentado, se debe alcanzar un compromiso entre el nivel de seguridad requerido y el tamaño de la firma. La solución elegida está basada en el esquema BLS propuesto en [BONEH2004] y en el esquema de firma BGLS [BONEH2003], que se va a presentar brevemente a continuación.

El esquema de firma agregada permite la creación de firmas sobre mensajes distintos $M_i \in \{0,1\}^*$.

El esquema incluye cinco algoritmos: generación de clave (*KeyGen)*, generación de firma *(Sign)*, verificación (*Verify)*, agregación (*Aggregate)* y verificación de agregación (*AggregateVerify)*. Los tres primeros son como los esquemas de firma ordinarios, los dos últimos son los que proporcionan la capacidad de agregación:

- **Generación de clave:** para un usuario concreto, tomar un número aleatorio $x \overset{R}{\leftarrow} \mathbb{Z}_n$, y computar $Q \leftarrow xP$. La clave pública del usuario será $Q \in G_2$, la clave secreta $x \in \mathbb{Z}_n$ y $P \in G_2$ será un parámetro público del sistema.

- **Firma:** para un usuario concreto, dada la clave secreta x y un mensaje $M \in \{0,1\}^*$, computar $R \leftarrow H(M)$, donde $R \in G_1$, y $\sigma \leftarrow xR$. La firma es $\sigma \in G_1$.

- **Verificación:** dada la clave pública Q de un usuario, un mensaje *M*, y una firma σ, computar $R \leftarrow H(M)$; aceptar si $e\ (\sigma, P) = e\ (R, Q)$.

- **Agregación:** para agregar un conjunto de usuarios $U \subseteq \mathbb{U}$, asignar a cada usuario un número de indexación *i*, numerándolos de 1 hasta $k = |U|$. Cada usuario $u_i \in U$ aportará una firma $\sigma_i \in G_1$ de un mensaje $M_i \in \{0,1\}^*$ de su elección. Los mensajes M_i deben ser todos distintos. Computar $\sigma \leftarrow \sum_{i=1}^{K} \sigma_i$. La firma agregada será $\sigma \in G_1$.

- **Verificación de la agregación:** Dada una firma agregada $\sigma \in G_1$ para un subconjunto de usuarios de agregación *U*, indexados de la forma indicada en el punto anterior, y dados los mensajes originales $M_i \in \{0,1\}^*$ y las claves públicas $Q_i = x_i P \in G_2$ para todos los usuarios $u_i \in U$. Para verificar la firma agregada σ,

    1. asegurar que los mensajes M_i son todos distintos, y rechazar en caso contrario; y
    2. computar $R_i \leftarrow H(M_i)$ para $1 \leq i \leq k = |U|$, y aceptar si $e(\sigma, P) = \prod_{i=1}^{k} e(R_i, Q_i)$.

La comprobación de que la firma agregada es correcta se realiza mediante la siguiente verificación. Cada usuario u_i tiene una clave secreta $x_i \in \mathbb{Z}_n$ y una clave pública $Q_i = x_i P$. La firma de cada usuario u_i, si está correctamente construida (es decir $\sigma_i = x_i R_i$, donde R_i es el *hash* del mensaje M_i que ha elegido el usuario), nos lleva a que la firma agregada σ es por tanto $\sigma = \sum \sigma_i = \sum x_i R_i$. Haciendo uso de las propiedades de las aplicaciones bilineales, desarrollando el lado izquierdo de la ecuación de verificación:

$$e(\sigma, P) = e\left(\sum x_i R_i\ , P\right) = \prod_i e(R_i, P)^{x_i} = \prod_i e(R_i, x_i P) = \prod_i e(R_i, Q_i).$$

La característica más destacable de estos sistemas es que con claves más reducidas ofrecen niveles de seguridad equivalentes a los criptosistemas de clave pública más extendidos basados en el problema de factorización de números grandes, como RSA, o en el problema del logaritmo discreto, como DSA. En la Tabla 2-4, se muestran los tamaños de claves recomendados por el *National*

Institute of Standards and Technology (NIST) usados en algoritmos convencionales de cifrado como DES y AES junto con los tamaños de claves para RSA, Diffie-Hellman y curvas elípticas que son necesarios para proveer un nivel equivalente de seguridad [NSA2009].

Tamaño clave simétrica (bits)	Tamaño clave RSA y Diffie-Hellman (bits)	Tamaño clave Curvas Elípticas (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

Tabla 2-4. Tamaños de claves recomendadas por el NIST para niveles de seguridad equivalentes [NSA2009].

Un parámetro importante de las curvas elípticas es su grado de seguridad (*embedding degree*). En un grupo G=<P> de una curva $E(\mathbb{F}_q)$, se dice que tiene un grado de seguridad k con respecto a l, si k es el entero más pequeño tal que $l \mid q^k-1$ donde l es de orden de G.

Cuando se selecciona una curva para ser utilizada en un criptosistema de curvas elípticas, se busca que tenga un grado de seguridad k tan grande como sea posible (siempre que no dificulte en exceso el cálculo con puntos de la curva), para evitar el ataque MOV [MENEZES1993].

Finalmente señalar que la criptografía basada en curvas elípticas está encontrando múltiples aplicaciones, y la podemos encontrar en dispositivos cotidianos que nos rodean: como el Windows Media Player para proteger las claves de las licencias que permiten la reproducción de contenidos protegidos con DRM2; los reproductores de *Blu-Ray* y la consola *Play Station* 3 llevan incorporada esta tecnología para para evitar la copia ilegal del software, la consola de Nintendo *Wii* basa en las curvas elípticas la seguridad de salvar las partidas "en la nube".

Otros dispositivos de menos potencia de cálculo que los anteriormente citados también hacen uso de esta tecnología, como ejemplos se pueden citar: los

teléfonos *BlackBerry*, que cifran con esta tecnología la información que transmiten.

3. Sistema propuesto.

3.1. Planteamiento teórico inicial

El problema al que da solución el sistema propuesto, podría plantearse en los siguientes términos: supongamos que en la fabricación de un determinado producto intervienen tres empresas A, B y C, cada una con su propio sistema de fabricación. Al finalizar cada una de las fases de producción, se realiza una verificación de los parámetros de calidad que deben cumplirse en esa parte del proceso. Un agente de control autorizado realiza la verificación y si es correcta, introduce los datos en el sistema. Cuando el producto acaba su proceso de fabricación en A, entre en la cadena de producción de B y se repite el proceso. Lo mismo para C.

Lo que se quiere conseguir es que al acabar el proceso, seamos capaces de verificar con una sola operación criptográfica que el producto ha superado todos los controles de calidad, que dichos controles han sido realizados por personal autorizado y que los datos de fabricación del producto no han sido alterados.

En el caso de que un producto informado favorablemente no cumpla los requisitos de calidad, debe poderse identificar el operario que cometió un error cuando verificó el producto.

Teniendo en cuenta lo anterior, el sistema propuesto debe dar solución a los siguientes retos:

1. Debe permitir de una forma sencilla integrar piezas o productos con calidad verificada de diversas procedencias en una cadena de producción final de la que saldrá el producto terminado. Por tanto debe contemplarse la relación entre empresas.
2. Debe permitir identificar el agente de control que ha verificado un determinado parámetro del producto y ha introducido el atributo correspondiente en el sistema, así como garantizar que sólo los agentes autorizados pueden introducir datos en el sistema.
3. Se deben contemplar, analizar y gestionar las relaciones de confianza presentes en el proceso completo de fabricación: entre empresas, entre una empresa y sus agentes de control, y entre el cliente y el producto finalizado.
4. El sistema será capaz de revisar periódicamente y de forma automática la confianza en los agentes de control, en función del correcto desempeño de su tarea.

5. Deberá incluir un sistema de gestión de la identidad de los agentes de control.
6. Utilizará un soporte físico que acompañará al producto donde se almacenarán los atributos más importantes del producto, así como la identidad y la firma del agente de control que los ha comprobado.
7. Deberá poder adaptarse a las limitaciones del soporte físico y del entorno de trabajo.

La solución propuesta se basa en el establecimiento de una identidad digital certificada de los productos basada en sus atributos, que serán verificados e incorporados al sistema sólo por agentes autorizados y autenticados, todo ello mediante el uso de una infraestructura de clave pública. Por tanto, lo que se consigue es poder identificar inequívocamente cada producto mediante una identidad de calidad certificada y verificable (principal diferencia con otros sistemas).

Además, el sistema propuesto es adaptable y por tanto aplicable a cualquier proceso productivo sujeto a un sistema de trazabilidad o control de calidad, cuyo flujo de trabajo conste de diferentes fases con puntos de control.

En el esquema presentado en la Fig. 3-1, en cada punto de control, representado por una lupa, se realizará la comprobación de los parámetros de calidad requeridos para que el producto pueda pasar a la siguiente fase de producción. En el historial de trazabilidad del producto, junto con los datos registrados también se adjuntará la firma electrónica del agente autenticado que ha realizado la verificación, teniendo así localizado al responsable de la información.

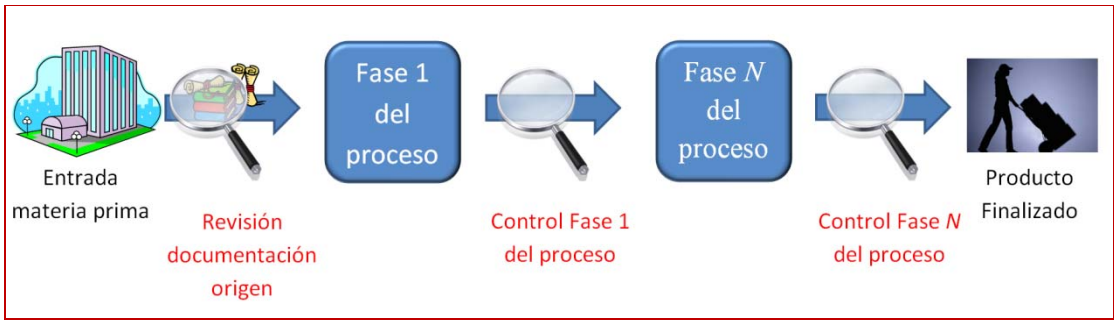

Fig. 3-1. Descripción del proceso

Otro aspecto a tener en cuenta es que el sistema propuesto contempla tanto que los agentes de control sean personal propio de la empresa como personal de una entidad de verificación externa. También puede trabajar con un sistema mixto, en el que convivan ambos tipos de agentes de control.

La herramienta básica que se utilizará para la validación de cada uno de los atributos es la firma digital del agente de control, que estará almacenada en un soporte físico que acompañará al producto durante toda la cadena de valor. Como ya se ha mencionado, el uso de la certificación digital a partir de esta firma lleva implícito el uso de una infraestructura de clave pública (PKI, *Public Key Infrastructure)* para jerarquizar las autoridades confiables [ROMAN2009].

Para garantizar la calidad de un producto a través de su cadena de producción, se establecerán unos puntos de control intermedios en los que se verificará dicha calidad. Pero esta garantía de calidad es global, es decir, se considera al producto como una "unidad", y por tanto se debe descartar cualquier producto que no supere un punto de control, por ello se debe ver al conjunto de firmas como un sello indivisible tanto de la calidad del producto como de su propia identidad.

A modo de ejemplo, en la Fig. 3-2 se presenta el proceso general de construcción de la identidad de un producto. En este ejemplo, se ha utilizado como soporte físico para almacenar los atributos y las firmas una etiqueta RFID:

- El producto empieza la cadena de valor con la fijación de una etiqueta inicializada para la escritura, que se generará en el primer punto de control.

- En cada punto de control se comprueban las firmas anteriores (caso de haberlas). Si la verificación es negativa se descarta el producto, y en caso contrario se procede a la comprobación de la calidad del producto.

- Si el producto alcanza la calidad requerida se añade el atributo correspondiente a la identidad y se firma digitalmente por el agente autenticado en el punto de control. En caso contrario, se descarta el producto.

- Este proceso se repite al finalizar cada una de las fases en las que se requiera la verificación de calidad.

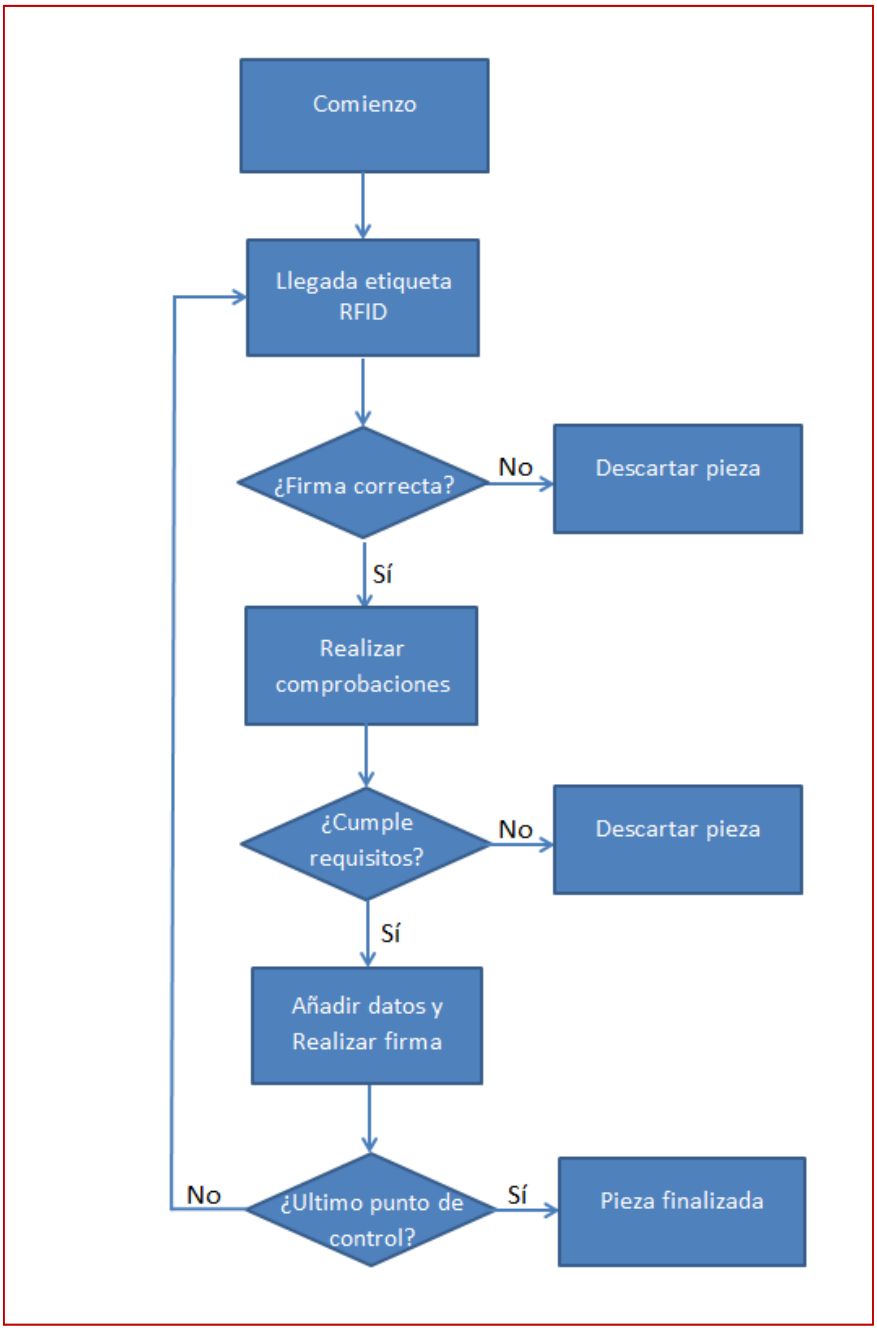

Fig. 3-2. Ejemplo de un proceso de construcción de identidad con calidad

Por tanto, la verificación de la calidad es una mera comprobación de la identidad del producto, definida entre todos los puntos de control y avalada por las firmas de los agentes de control. Esta forma de trabajar con la información de control en el proceso productivo, permite verificar la calidad de los productos hasta ese momento en cualquier punto del proceso, de una forma rápida y sencilla.

Considerando la construcción de la identidad como un proceso aditivo, la escalabilidad del sistema es sencilla, ya que el número de puntos de control puede ser repetido *n* veces sin necesidad de realizar ningún cambio estructural en el sistema.

Dado que los atributos que conforman la identidad van firmados por el agente de control que los verificó, es necesario un sistema de control de confianza, que decida si un agente controlador es merecedor de la confianza para realizar esta tarea, lo que conlleva permitirle el acceso o no al sistema de información y a su clave privada de firma electrónica. Así mismo también se debe considerar la confianza entre la empresa productora y un regulador centralizado (que garantice las transacciones entre diferentes empresas involucradas en una cadena de suministro) y finalmente la confianza del cliente en un producto adquirido.

Notar, que una aportación importante del sistema es que la calidad de todo el proceso puede comprobarse mediante una sola verificación de firma.

En el resto del capítulo, se va a presentar descripción de la prueba de concepto, donde se mostrarán los sistemas de confianza, gestión de la identidad y seguridad, así como una representación de los flujos de información.

3.2. Prueba de concepto

Tras el planteamiento teórico mostrado en el apartado anterior, en este apartado se describe el planteamiento teórico de la prueba de concepto, así como los resultados de su implementación en un sistema de trazabilidad alimentaria de un producto manufacturado, concretamente de piezas de jamón serrano con denominación de origen "Jamón de Teruel". En este caso se identifica al producto mediante un número identificativo único y atributos físicos, los cuales son almacenados en una etiqueta RFID y certificados mediante una infraestructura de clave pública.

A continuación se van a presentar los modelos elegidos y los sistemas desarrollados para la implementación y gestión de la identidad digital de calidad, así como de las diversas relaciones de confianza que se dan en el proceso. Finalmente se presentará una reflexión de cómo el sistema puede ayudar a detectar fraudes en la autenticidad de un producto y un resumen de los flujos de información durante el proceso de elaboración del mismo.

3.2.1. Sistema y relaciones de confianza

Tras la revisión de bibliografía realizada en el apartado 2.1.3, se concluyó que el tipo de modelo más adecuado al entorno de trabajo en el que se enmarca esta tesis es un sistema de confianza basado en la propia experiencia y en la observación de las relaciones de los miembros de la comunidad entre sí.

De los modelos revisados, el mayor problema que presentan de cara al contexto de nuestra prueba de concepto, es que están muy orientados al comercio electrónico y a su uso en agentes computacionales. En nuestro caso esta aproximación no es la más adecuada, ya que es posible establecer un contacto previo con las entidades implicadas, realizar las comprobaciones pertinentes, acordar los compromisos legales oportunos y por tanto es posible establecer a priori un marco de confianza con un nivel elevado de fiabilidad. El modelo más cercano a las necesidades del sistema planteado es el de Kuhlen[13] [KUHLEN1999], si bien no acaba de adaptarse plenamente, por lo que se propone un sistema nuevo, que se expondrá a continuación. El sistema propuesto también comparte algunos rasgos con los modelos *Sporas* e *Histos* [ZACHARIA1999], como la reputación inicial baja y su aumento con el tiempo si el comportamiento del agente es satisfactorio. Estas ideas se han adaptado a las necesidades y características específicas de los entornos industriales de producción.

Aunque tradicionalmente los controles de calidad solían ser realizados por una entidad externa, la tendencia actual en los procesos de control de calidad y trazabilidad, es que estos controles sean realizados por personal de la propia empresa productora y luego, una vez finalizado el proceso, sean verificados por la entidad externa, normalmente por procedimientos de muestreo. De este planteamiento se derivan dos delegaciones de confianza: una primera entre la entidad externa (por ejemplo un Consejo Regulador de una Denominación de Origen Protegida) y la empresa productora de un alimento amparado por la denominación; y una segunda que se produce entre la empresa y el empleado (o el instrumento) encargado de realizar los controles de calidad, lo que hemos denominado el agente de control.

En vista de lo anterior, en el sistema que se propone en esta tesis, se van a considerar ambas relaciones de confianza:

---

[13] *Señalar que este modelo se encuentra descrito en alemán, y la información sobre él ha sido obtenida de la revisión realizada por Pinyol y Sabater en [PINYOL2011].*

1.- Entre empresas y un ente regulador centralizado.

2.- Entre agentes de control y la empresa productora.

También se va a presentar brevemente una tercera relación de confianza, que si bien no afecta al proceso de fabricación del producto propiamente dicho, es muy importante, ya que es la confianza que tiene el cliente en el producto adquirido.

A continuación, se van a desarrollar las relaciones de confianza expuestas anteriormente, y que integran el módulo de gestión de confianza del sistema. Antes de continuar, conviene recordar[14] que se entiende por confianza una "medida acerca de la certeza que se tiene en que otro agente será capaz de ejecutar eficientemente una determinada acción, teniendo en cuenta su propio conocimiento" [CABALLERO2008].

3.2.1.1. Confianza empresa – regulador centralizado

En este tipo de relación, el nivel de confianza en la empresa productora es establecido por el personal del organismo regulador, tras analizar los datos aportados por la empresa, realizar las comprobaciones oportunas y verificar que cumple los requisitos establecidos. Si la evaluación es positiva, se le otorga un nivel de confianza "1", es decir se autoriza a la empresa solicitante a producir bajo el paraguas de marca que gestiona el ente regulador.

Podemos representar al regulador centralizado como una "caja negra" que tras recibir y procesar todos los *inputs* de la solicitud emite un resultado: "1" si se integra al solicitante en el sistema y "0" si es rechazado por no cumplir algún requisito. Realmente, se está asociando confianza con el cumplimiento de unos requerimientos. Posteriormente se establecerá un procedimiento de control para llevar una verificación periódica o bajo demanda del cumplimiento de los requisitos.

El proceso pude verse representado esquemáticamente en la Fig. 3-3 .

[14] *como ya se indicó en el capítulo 2.*

Fig. 3-3. Esquema de confianza empresa - regulador

Si el resultado es "0" el solicitante podrá repetir el proceso una vez subsane las carencias o problemas detectados. Si el resultado es "1" el solicitante ingresará en el sistema.

Se establecerán mecanismos de control y revocación de confianza, para garantizar el cumplimiento de los requisitos a lo largo del tiempo.

Las entidades en las que se confía, podrán integrar la identificación y claves públicas de sus agentes de control en un repositorio centralizado, gestionado por el organismo regulador y accesible por el resto de integrantes que producen bajo el amparo del regulador. Notar que este regulador puede crearse ad-hoc entre las empresas implicadas en un proceso de fabricación, lo que permite una aplicación sencilla del sistema en múltiples entornos.

3.2.1.2. Confianza agentes de control – empresa productora

Una vez que una empresa productora ha sido admitida en el sistema, debe garantizarse que se mantenga la calidad mínima requerida por la marca bajo la que se ampara la producción, por ello se tiene la necesidad y la obligación de establecer mecanismos de control para verificar el cumplimiento de los requisitos acordados. El sistema de verificación que se propone se basa en agentes de control.

Desde el regulador centralizado, se realiza una delegación de atribuciones a una serie de agentes que se encargarán de realizar las comprobaciones y verificaciones correspondientes y emitir un informe sobre el cumplimiento de los requisitos. Aunque tradicionalmente estos agentes de control eran personal del organismo regulador, actualmente la tendencia parece ser que los agentes

responsables del control puedan ser trabajadores de las propias entidades controladas. El sistema que se propone en esta tesis para establecer la confianza en los agentes, puede ser utilizado en ambos casos, tanto si los controladores pertenecen a la empresa como si no. Una tercera opción es una solución mixta, donde se den ambos tipos de controladores, caso que también puede ser abordado sin ninguna modificación por el sistema propuesto.

Como ya se ha comentado anteriormente, ver Fig. 3-1, durante el proceso de fabricación se establecen unos puntos de control o *checkpoints*, donde se verifica el cumplimiento de unos requisitos mínimos, mediante la realización de las comprobaciones oportunas. Una vez realizadas dichas comprobaciones, el agente que las ha realizado emite un informe que firma, o lo que es lo mismo, añade atributos a la identidad digital de producto. Con el sistema propuesto, se garantizan dos cosas:

- La primera: que el agente encargado de realizar la validación está autorizado para ello. Esto se puede garantizar mediante la utilización de un proceso de autenticación, que tras su superación le permitirá acceder a un repositorio donde se encuentra depositada su clave secreta con la que podrá firmar electrónicamente el atributo. Por tanto, sólo los agentes autorizados podrán firmar las validaciones de los productos.

- La segunda: que los datos introducidos en el sistema sobre las características del producto están respaldados por un agente que ha firmado los datos. Esto permite tener un mayor nivel de confianza en los atributos, ya que han sido comprobados por una entidad que se responsabiliza de ellos, identificable y que previamente ha sido objeto de una delegación de confianza y de un proceso de autenticación.

Como se desprende del párrafo anterior, se delega en los agentes de control la tarea de verificar una serie de atributos de los productos, pero a su vez, estos agentes verificadores también son controlados y disponen de un nivel de reputación.

A continuación, se va a definir el nivel de confianza y su relación dinámica con el nivel de reputación, que se irá actualizando a lo largo del tiempo en función del comportamiento de los agentes.

El valor de confianza, C, es booleano y representa la decisión final de si se confía en el agente o no, de acuerdo a la siguiente codificación de valores:

- el valor "1" representa un agente en el que se confía y por tanto los datos por él verificados son tomados como verdaderos. Inicialmente un agente que ha sido introducido en el sistema tiene un valor de confianza "1".

- el valor "0" representa un agente en el que se ha dejado de confiar, y por tanto se le revoca el acceso a la clave de firma para que no pueda introducir más datos en el sistema. Lo que hace que un agente cambie su nivel de confianza de "1" a "0" es que su reputación actual, R_{ACT}, sea igual o menor que cero.

$$C = \begin{cases} 1 \; si \; su \; nivel \; de \; reputación \;\; alcanza \; unos \; mínimos \\ 0 \; si \; su \; nivel \; de \; reputación \; no \; alcanza \; unos \; mínimos \end{cases} \quad (3\text{-}1)$$

Como ya se anticipó en el apartado 2.1.2, se utiliza la confianza como una medida acerca de la certeza que se tiene en que un agente de control ejecutará eficientemente el control e introducción en el sistema del atributo del que sea responsable, teniendo en cuenta el número de fallos en su tarea a lo largo del tiempo.

En la ecuación (3-1), se puede apreciar que la confianza está relacionada con el nivel de reputación[15], es más, en este caso sólo depende de ese parámetro. Por tanto es extremadamente importante llevar un adecuado seguimiento de la reputación a lo largo del tiempo, que permita tener su valor actualizado.

Para este apartado, se han estudiado algunos sistemas de gestión de confianza e incentivos, con aplicaciones en diversos ámbitos: seleccionar los nodos con los que interactuar en una red Ad Hoc móvil [CHO2011], elegir rutas seguras [GONZALEZ2011], establecer niveles de confianza en redes P2P [KAUR2012,EL-HALEEM2010], confianza en vendedores en sistemas comercio electrónico [ZHANG2009], políticas de incentivos para mejorar la productividad de operarios o sistemas de economía de fichas utilizados en sicología para cambiar comportamientos.

[15] *1. Es una evaluación basada en la historia de interacciones con (u observaciones de) una entidad, ya sean realizadas directamente por el evaluador o transmitidas por un testigo [JØSANG2007]. 2. Certeza que un agente tiene sobre el comportamiento de otro, compuesta a partir del conocimiento que es capaz de extraer de las relaciones con el resto de agentes, ya sea por el análisis de la red de relaciones sociales como por la información suministrada por otros" [CABALLERO2008].*

Dado que cada tipo de modelo se ajusta a una tarea muy concreta, ninguno acababa de encajar con nuestras necesidades. Por ejemplo, en muchos de los modelos de gestión de confianza estudiados (redes ad-hoc, enrutamiento seguro, comercio electrónico), una de las tareas más complicadas a las que se deben enfrentar los agentes es obtener el nivel de confianza de sus vecinos, para ver cuanta credibilidad le dan a la información que éstos les aportan, cosa que no es excesivamente útil en nuestro caso. Por ello, se planteó para gestionar la confianza en los agentes de control, la utilización de un sistema inspirado en una cubeta con goteo o *Leaky Bucket*, utilizada en redes de computadores para conformar el tráfico de red. Este algoritmo fue propuesto por primera vez por Turner [TURNER1986].

La variante de este algoritmo en la que se inspira nuestro sistema, es la de cubeta con *tokens* (descrita en [TANENBAUM2010]), en la cual una cubeta se va llenando con fichas o *tokens*. Su funcionamiento es muy intuitivo, podemos imaginar una cubeta de capacidad finita, C, que en un momento dado está llena. A partir de ese momento, la cubeta se va llenando de fichas, a una velocidad de ρ fichas por segundo (tasa de reposición). Simultáneamente, se "abre" la salida de la cubeta y las fichas se irán consumiendo a la velocidad máxima de salida, M fichas por segundo, hasta que la cubeta se vacíe completamente. Una situación concreta en este proceso, queda expresada en la siguiente fórmula:

$$C + \rho S = MS \quad (3\text{-}2)$$

En la expresión (3-2), S representa el tiempo transcurrido desde que se ha "abierto" el grifo de la cubeta, y permite calcular los parámetros (C y ρ) adecuados para poder transmitir a una tasa máxima constante durante un número determinado de segundos.

Con este algoritmo lo que se consigue es una conformación del tráfico de una red de manera más eficiente que la cubeta con goteo, que consigue transformar un tráfico a ráfagas en uno periódico, y por tanto más constante y predecible. Con *Token Bucket* lo que se persigue es que si durante cierto tiempo no ha habido tráfico (no ha habido salida de fichas) la cubeta se habrá ido llenando a la velocidad de la tasa de reposición ρ, y por tanto cuando llegue una ráfaga se permitirá su salida a máxima velocidad, M, durante un tiempo S, hasta que se vacíe la cubeta:

$$S = \frac{C}{M - \rho} \quad (3-3)$$

de esta manera se consigue que un enlace funcione de manera más eficiente. Al llevar un control del tráfico que se ha enviado por ese enlace en el periodo de tiempo inmediatamente anterior, es posible durante algunos segundos la transferencia de una ráfaga a máxima velocidad.

A partir de este algoritmo, se va a establecer una analogía con la reputación de un agente que está verificando productos. En este caso las fichas que hay en la cubeta van a representar su reputación actual, R_{ACT}. El nivel de reputación irá subiendo conforme se verifican productos de forma correcta. Este proceso se va repitiendo hasta llegar a la capacidad máxima de la cubeta, que en este caso se denominará R_{MAX}. La introducción de este valor límite, R_{MAX}, responde a la necesidad de limitar el valor de reputación de un agente, para que aunque durante un tiempo su comportamiento sea intachable, no pueda alcanzar un nivel de reputación tan elevado, que no le afecten prácticamente las penalizaciones. Un ejemplo cotidiano de sistema de reputación con valor máximo, es el permiso de conducir por puntos[16] actualmente vigente es España.

Paralelamente, en cualquier momento se puede producir un descenso del número de fichas de la cubeta. En nuestro caso, las fichas se consumirán cuando se detecte un error (sería el equivalente a una ráfaga de datos de una duración determinada a una tasa de datos concreta), lo que hará que el agente pierda reputación.

En el caso que nos ocupa, deberemos disociar el valor de tiempo que aparece a ambos lados de la ecuación, ya que en la fórmula original mientras se producía la transmisión de datos a máxima velocidad, es decir mientras se vaciaba la cubeta, se iban reponiendo las fichas, estando su generación asociada al tiempo común a ambos lados de la igualdad. La primera conversión que realizaremos será:

$$C + \rho S_1 = M S_2 \qquad (3\text{-}4)$$

donde C representa la capacidad máxima de la cubeta, ρ es el número de fichas que se generan por cada pieza verificada correctamente, S_1 es el número de piezas verificadas correctamente, S_2 el número de piezas verificadas erróneamente y M el número de fichas que se pierden por cada verificación errónea. Observar que la fórmula anterior, (3-4) no es útil todavía, ya que al disociar el parámetro común S, en dos parámetros independientes, deja de cumplirse la condición original que era que siempre que se generaban fichas también se consumían. Por ello, vamos a

[16] *http://www.dgt.es/portal/ca/oficina_virtual/permiso_por_puntos/*

buscar una fórmula que exprese mejor la realidad del proceso que se producirá en nuestro sistema. Vamos a renombrar las variables, para que sea más intuitiva la comprensión del proceso:

- Pasamos a denominar Reputación máxima, R_{MAX}, a C.
- Pasamos a denominar Piezas verificadas correctamente, P_{VC}, a S_1.
- Pasamos a denominar Piezas verificadas erróneamente, P_{VE}, a S_2.
- El factor de penalización, FP, sustituirá a M.
- La tasa de reposición ρ, sigue manteniendo su nombre, pero ahora son fichas generadas por pieza verificada correctamente (en lugar de por unidad de tiempo).

Si introducimos una nueva variable, R_{ACT}, que es el contador que nos da en cada instante el nivel de reputación, es decir el nivel de la cubeta, tenemos que:

$$R_{ACT} = \rho \cdot P_{VC} - FP \cdot P_{VE} \qquad (3\text{-}5)$$

A la vista de esta expresión, todavía debemos incorporar dos condiciones importantes:

- La posibilidad de otorgar un nivel de confianza inicial, R_{INI}, a un agente nuevo en el sistema,
- y asegurar que R_{ACT} sea siempre menor o igual que R_{MAX}.

Con todos estos factores, construimos el siguiente algoritmo en pseudocódigo, para establecer el valor de R_{ACT}:

$R_{ACT}=R_{INI}$

Mientras $R_{ACT}>0$ *Hacer*

{

$R_{ACT}= R_{ACT} + \rho \cdot P_{VC} - FP \cdot P_{VE}$

$R_{ACT}= min \{R_{ACT}, R_{MAX}\}$

Fin Mientras}

Fin

Es decir, en un instante dado el valor de reputación actual será la suma del valor de reputación inicial más las fichas conseguidas por verificaciones correctas menos las fichas perdidas por verificaciones incorrectas.

Recordando (3-1), tenemos que si $R_{ACT}>0$ la confianza, C =1, y por tanto confiamos en ese agente. En caso contrario, es decir si $R_{ACT} \leq 0$, C=0 y se deja de confiar en ese agente. Podemos introducir C en el algoritmo anterior:

$R_{ACT}=R_{INI}$

Mientras $R_{ACT}>0$ *Hacer*

{

$C=1$

$R_{ACT}= R_{ACT} + \rho \cdot P_{VC} - FP \cdot P_{VE}$

$R_{ACT}= min \{R_{ACT}, R_{MAX}\}$

Fin Mientras}

$C=0$

Fin

A la vista de todo lo anterior, en la siguiente tabla se presentan los parámetros más importantes del sistema, su abreviatura y una breve explicación de su función.

Abrev.	Parámetro	Función
R_{INI}	Reputación Inicial	Permite elegir la reputación otorgada a los agentes de control cuando entran en el sistema.
R_{MAX}	Reputación Máxima	Limitar el valor máximo de reputación de un agente.
R_{ACT}	Reputación Actual	Refleja la reputación actual del agente.
P_{VC}	Número de productos verificados correctamente	Contiene el número de productos verificados correctamente
$\boldsymbol{\rho}$	Constante	Indica en cuanto crece la reputación por cada producto verificado correctamente
N_{PV}	Productos verificados por día	Contiene el número medio de productos verificados en una jornada de trabajo
P_{VE}	Número de productos verificados erróneamente	Contiene el número de productos verificados erróneamente
FP	Factor de penalización	Indica en cuanto decrece la reputación por cada producto verificado erróneamente

Tabla 3-1. Parámetros del sistema de confianza

Las acciones que van realizando los agentes de control son registradas por el sistema, influyendo en la reputación actual, representada como R_{ACT} de la siguiente manera:

- **Productos validados correctamente**: se aumenta el valor de reputación actual un valor $P_{VC} \cdot \rho$, donde P_{VC} corresponde al número de productos verificados correctamente y ρ es una constante que se introducirá como parámetro en el sistema. Es decir,

$$R_{ACT} = R_{ACT} + (N_{PV} \cdot \rho) \qquad (3\text{-}6)$$

El valor de ρ permite ajustar cuantos días de trabajo sin errores necesita un agente para llegar al máximo valor de reputación:

$$\rho = \frac{R_{MAX} - R_{INI}}{N_{PV} \cdot d} \qquad (3\text{-}7)$$

donde N_{PV} es el número medio de productos validados en un día, y *d* el número de días que se desea que transcurran para que un operario, que no cometa ningún error de validación, pase del nivel de reputación inicial (R_{INI}) al máximo (R_{MAX}).

La actualización del valor R_{ACT}, aunque podría realizarse tras la validación de cada producto, por motivos de eficiencia operativa se realizará tras cada jornada de trabajo. Como se muestra a continuación, el valor R_{ACT} se verá fuertemente afectado cuando se detecten errores.

- **Productos validados incorrectamente:** se disminuye el valor de reputación actual en la cantidad resultante de la operación $(FP \cdot P_{VE})$, donde P_{VE} corresponde al número de productos verificados de manera incorrecta y *FP* es el factor de penalización que se introducirá como parámetro en el sistema.

  A priori, el número de errores[17] debería ser extremadamente bajo. Además, considerando el impacto tan importante que tiene en la imagen de marca que un producto de menor calidad que la programada llegue al consumidor, el descenso en el nivel de confianza sobre el agente debe ser importante. El valor de *FP* puede ser constante o variable, por ejemplo se puede tener en cuenta la confianza actual en el agente de control a la hora de penalizar.

El valor R_{ACT} se verá afectado por las validaciones incorrectas de la siguiente manera:

$$R_{ACT} = R_{ACT} - (FP \cdot P_{VE}) \qquad (3\text{-}8)$$

- **Productos validados de manera fraudulenta:** bajo la denominación "productos validados incorrectamente" se englobaban los errores involuntarios, que pueden aparecer en cualquier actividad humana. En el presente epígrafe, y a diferencia del anterior, se engloban las validaciones realizadas de mala fe. Si se detecta que un agente de control introduce datos incorrectos de forma intencionada, cosa no sencilla de demostrar, será expulsado del sistema.

[17] *Se recuerda, que se considera un error cuando una pieza que no debería haber pasado los controles en un punto de control, sigue el proceso como si cumpliera los requisitos. No tiene nada que ver con el número de productos descartados por no cumplir los requisitos fijados.*

> A partir del instante en el que el valor de confianza sobre un agente es cero, se le retirarán las atribuciones delegadas, en la práctica le será revocada la clave privada de firma y no podrá realizar más verificaciones (sin descartar cualquier otro tipo de medidas de otra índole que se puedan ejercer sobre él).

La evaluación de confianza se hará tras cada jornada de trabajo, una vez se haya procedido a la actualización de R_{ACT}. Cuando un agente se autentique en el sistema, se comprobará el nivel de confianza del agente y si es cero no se le permitirá el acceso al sistema. Además, el sistema avisará al responsable del agente con C=0, para que sea sustituido y este hecho no afecte al normal funcionamiento de la cadena de producción en la siguiente jornada. Al igual que con la reputación actual, podría realizarse la evaluación de la confianza de manera instantánea tras cada introducción de productos validados incorrectamente, aunque por motivos de eficiencia operativa no se ha optado por esta posibilidad.

Inicialmente el sistema se plantea como parte de un sistema de control de calidad a posteriori, es decir, inicialmente se presuponen todos los productos verificados de manera correcta, y cuando se detecten los errores se introducirá la información relativa en el sistema tan pronto sea posible. En la Fig. 3-4 se muestra un esquema de funcionamiento del sistema.

Los productos terminados se someterán a procesos estándar de control de calidad, ya sea del total de productos o por métodos de muestreo, y si se detectan fallos, una vez localizado el responsable, se introducirán los datos en el sistema para actualizar los valores de reputación y confianza de los agentes implicados.

El sistema también es válido para el caso de que los agentes que introducen los datos no sean humanos (por ejemplo básculas y sistemas de clasificación automática). No obstante, este tipo de errores en los sistemas automáticos de medida y clasificación van a ser prácticamente inexistentes y normalmente relacionados con averías en los equipos.

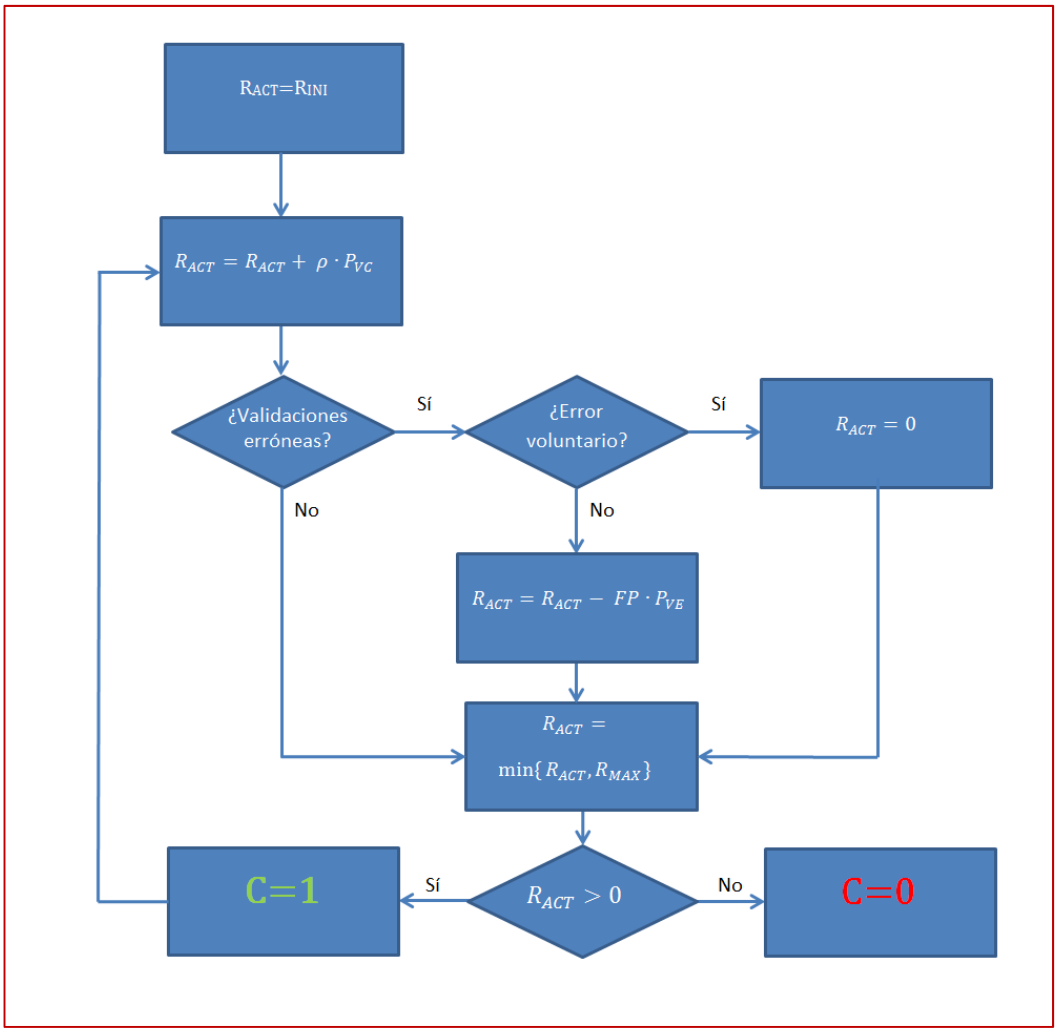

Fig. 3-4. Sistema de control de confianza en agentes

3.2.1.3. Confianza entre el cliente y un producto finalizado comercializado

Cuando el cliente elige un producto está valorando multitud de factores: precio, calidad del producto, imagen de la marca, confianza en un organismo regulador, etc… Por todo ello, es importante mantener unos altos niveles de calidad en los productos que llegan al consumidor.

Con el sistema propuesto, además de una serie de elementos reconocibles en el propio producto y que hacen factible su identificación como producto original, se incorporará una firma digital en la etiqueta del producto, que avalará que se han cumplido todos los requisitos y procesos necesarios para conseguir la calidad que el cliente espera y cuyo cumplimento controla el organismo regulador. De esta manera se refuerza la confianza del cliente en la marca del producto.

En el caso de un producto defectuoso y gracias a su identidad digital, se puede localizar no sólo el origen de la anomalía, sino saber qué personas o máquinas dieron por buenos ciertos atributos que finalmente se revelan falsos. Además, la utilización de marcadores de confianza, incrementa la confianza de los consumidores [LEE2007].

Los clientes pueden contribuir a detectar fraudes ya que cada producto tendrá, dentro de los atributos que conforman su identidad, un identificador único validado mediante un proceso de firma digital, y si el número aparece repetido o la firma no es correcta, existe una altísima probabilidad de que se trate de una falsificación del producto, hecho que podrán denunciar ante el organismo regulador.

3.2.2. Sistema de gestión de la identidad de los agentes de control.

Como ya se señaló en el capítulo segundo, el objetivo de la gestión de identidad puede abordarse desde dos perspectivas [LINDEN2009]:

- Desde el punto de vista técnico: asegurar que los usuarios sólo podrán realizar las acciones para las que han sido autorizados.
- Desde el punto de vista jurídico: asegurar que se pueda responsabilizar a una persona de las acciones realizadas bajo su identidad autenticada.

Así pues, en el sistema propuesto se busca cumplir ambas perspectivas, aunque de acuerdo con la clasificación de [CAO2010], el modelo de gestión de la identidad adoptado en el presente sistema será el modelo aislado, y desde el punto de vista paradigmático correspondería con un modelo centrado en el usuario (en este caso el usuario es el agente de control).

Una vez que una empresa productora ha recibido la confianza del ente regulador, y se ha integrado en el sistema, se instala en la empresa un proveedor de identidad, es decir, un servidor encargado de almacenar las claves privadas de firma de los agentes controladores.

Cuando han sido seleccionados los agentes controladores, se les crea una identidad en el sistema a la que se asocia un par de claves de firma, una privada que se mantendrá dentro del sistema y una pública que podrá ser difundida, y de hecho se almacenará en un repositorio accesible desde Internet.

Aunque inicialmente el proceso de autenticación utilizado en el prototipo se basa en el uso de *login* y *password*, no habría ningún inconveniente para realizar este control mediante métodos de autenticación más seguros, como el uso de tarjetas inteligentes securizadas, parámetros biométricos o sistemas combinados.

Una vez realizada la autenticación, el sistema comprobará en la base de datos el nivel de confianza depositado en el agente de control. Si el valor es un "1" le dará acceso al sistema y podrá validar las piezas en su punto de control, en caso contrario no se le dará acceso al sistema.

3.2.3. Autenticidad del producto

Una de las ventajas de utilizar la identidad digital de calidad propuesta en esta tesis, es que permite proteger y garantizar la autenticidad del producto y la veracidad de los diferentes parámetros de calidad inspeccionados por agentes autorizados.

En este entorno, y tras estudiar el proceso de producción que se desarrolla en recintos cerrados y con el acceso perfectamente controlado, se deben identificar cuáles son las amenazas. En este sentido, siguiendo el desarrollo de modelo de ataques descrito en [SONG2011] se identifican dos tipos de atacantes:

1. *Externo:* un productor que no pertenece al regulador que intenta vender sus productos como si hubiesen pasado todos los controles de calidad que acredita la etiqueta. Para conseguir su objetivo, deberá poder generar etiquetas falsas que pasen correctamente el proceso de verificación de las mismas.
2. *Interno:* en este caso, el atacante es un agente de control que actúa de manera fraudulenta. El agente de control quiere boicotear la producción de calidad evaluando positivamente productos que no superan el umbral mínimo de calidad prestablecido.

Ambos casos son teóricamente detectables. El primer caso porque la información de la etiqueta no coincide con la identidad del producto, y en el segundo caso el atacante será detectado por el sistema de evaluación de confianza agente de control – empresa productora. En ambos casos, cualquier solución debe ser siempre a posteriori, una vez que se haya producido la incongruencia en el etiquetado o el sistema retire la confianza a un agente. Por tanto, el objetivo de las medidas de seguridad que se construyan en defensa del producto será localizar el punto de fraude e identificar su origen.

Por otra parte, aunque la detección del fraude teóricamente es sencilla, en la práctica puede ser mucho más complicado de detectar si esta incongruencia en el etiquetado sólo es palpable con instrumentos de medida de cierta precisión. Para paliar esta dificultad y dado que la detección del producto fraudulento es siempre a posteriori, estas medidas tecnológicas han de estar complementadas con un adecuado método de muestreo para el control del producto comercializado.

Se propone la utilización de una infraestructura de clave pública para criptografía de firmas agregadas con criptografía de curva elíptica (ECC, *Elliptic Curve Cryptography*) [MENEZES 1994]. Una de las características de la ECC es que se puede conseguir un nivel de seguridad equivalente al de otros métodos criptográficos con una longitud de firma menor [LENSTRA2001].

3.2.4. Flujos de comunicaciones

La aplicación del modelo a un sistema de trazabilidad es flexible en el modo de realizar las verificaciones: puede realizarlas tanto en modo *online* como *offline*. Además, ofrece varias opciones a la hora realizar la implementación de la PKI necesaria para el funcionamiento del sistema. Todas estas alternativas van a permitir que el sistema se adapte a las necesidades particulares de la cadena de suministro, o incluso a los requisitos específicos de cadenas de montaje o de producción.

La única restricción que presenta el sistema, dado que la identidad se almacena en una etiqueta RFID que acompaña al producto, es la necesidad de que en cada punto de control exista un lector/grabador RFID para interactuar con las etiquetas. Partiendo de esta base, el resto del sistema es adaptable a las necesidades del entorno en el que se vaya a implantar. Cada uno de los puntos de control tendrá que disponer de un dispositivo de procesado y comunicación para establecer la comunicación tanto con el dispositivo RFID como con la base de datos o sistema *back-end*. El dispositivo en cuestión será normalmente un ordenador o terminal, pero también se podrían utilizar PDAs (*Personal Digital Assistant*), ordenadores portátiles o *smartphones* para llevar a cabo esta tarea.

El canal de comunicación podrá ser cableado o inalámbrico. Dependerá tanto de las condiciones del entorno en el que se desarrollen los controles como del tipo de dispositivo que realice el procesado de datos. En el caso de entornos industriales como el que nos ocupa, el canal suele ser cableado, ya que los sistemas inalámbricos pueden sufrir problemas tanto por las interferencias

electromagnéticas generadas por la maquinaria de producción, como por la dificultad de propagación de las ondas electromagnéticas debida a la alta humedad ambiental inherente a ciertos procesos productivos.

Dentro del sistema de trazabilidad, el apartado que permite una mayor versatilidad de implantación es la PKI. Se podrá implementar de manera distribuida, semi-distribuida o centralizada [OZSU1991]. La manera más habitual es utilizar un servidor como repositorio de claves públicas, que no tiene por qué ser el mismo que albergue la base de datos, al que se conectarán los diferentes dispositivos para realizar la verificación de las firmas. Si además se diseña el sistema de forma que las claves privadas de cada usuario estén almacenadas también en el servidor, y que se realicen en él las operaciones de firma, estaremos hablando de un sistema centralizado, como se muestra en la Fig. 3-5.

El sistema semi-distribuido varía del centralizado en el almacenamiento de las claves privadas. El repositorio de claves públicas se encuentra en el servidor central y es éste el encargado de proveerlas a los dispositivos o, incluso, realizar las verificaciones, mientras que las claves privadas de los usuarios estarán almacenadas en los dispositivos de manera individual, no quedando almacenadas en el servidor. De esta manera, la firma de los mensajes se realiza de manera local y después es enviada al servidor para que los nuevos valores sean almacenados en la base de datos.

Por último, se puede instalar el sistema de forma distribuida [CAPITANI2011]. La gestión de las claves privadas y el proceso de firma es el mismo que en el caso anterior, diferenciándose de éste en el tratamiento de las claves públicas. En el sistema distribuido, sigue existiendo un repositorio de claves públicas, pero no se utiliza para realizar las verificaciones de las firmas. Cada terminal individual almacena una copia del repositorio de claves públicas y es el propio terminal el encargado de realizar las verificaciones de las firmas. Tan sólo deberá conectarse con el repositorio central para aquellos casos en los que su repositorio local no tenga la clave pública de alguno de los firmantes. En ese caso, se conectaría al repositorio central para obtener y almacenar la clave pública que desconocía.

Además de las diferencias entre los distintos métodos de implantación respecto al tipo de red y dispositivos empleados, existen otras consideraciones importantes a tener en cuenta respecto al procesado de los datos que se debe hacer en cada uno de ellos. El sistema centralizado carga todo el procesado en el servidor central. Esto libera a los terminales de carga computacional y por tanto

pueden ser dispositivos con unos requisitos operativos muy básicos. Mientras, el servidor central tendrá unos requisitos que, aunque variarán de un sistema a otro, serán elevados para poder llevar a cabo todo el procesamiento necesario. Otra característica es que la clave privada, al estar almacenada en el propio servidor, será más difícilmente exportable y, dependiendo de los escenarios en que se implante el sistema de trazabilidad, pueda dar una sensación de menor seguridad.

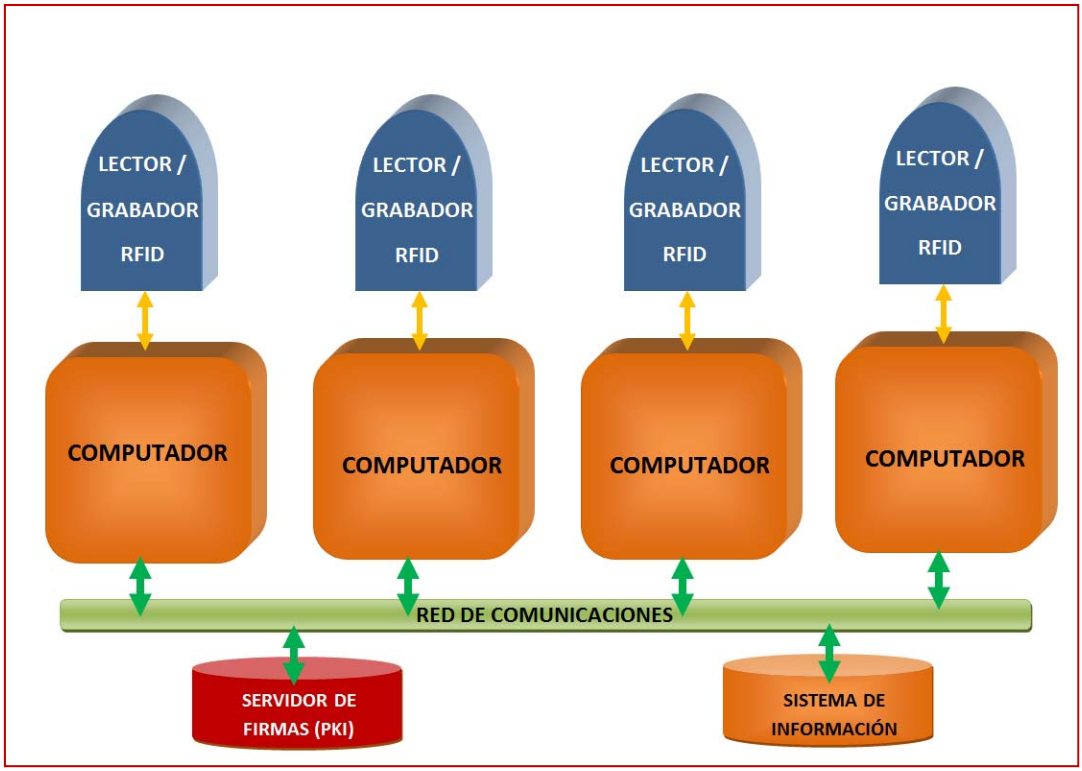

Fig. 3-5. Sistema centralizado de gestión de firmas

El sistema semi-distribuido, permite liberar al servidor central de realizar las firmas de los mensajes. Dependiendo de la configuración seleccionada también podrán ser los terminales los encargados de realizar las verificaciones. Lo que implica menos carga computacional para el servidor central, pero mayor para los terminales.

El sistema distribuido minimiza la carga de trabajo en el servidor central de claves. Este sistema permite además trabajar de manera offline siempre que el repositorio local esté actualizado. Implica que toda la carga computacional recae sobre los terminales y el servidor de claves públicas es un simple repositorio de consulta.

4. Diseño, prototipo y resultados

En este capítulo se van a mostrar las decisiones de diseño aplicadas al sistema, y su implementación en un prototipo que ha servido como base de pruebas y sobre el cual se han obtenido los resultados de viabilidad del sistema.

En primer lugar se presenta una revisión de los requisitos del sistema, para luego pasar a la elección del tipo de curva elíptica a utilizar y sus parámetros. Posteriormente se muestra la implementación de la aplicación y la seguridad aportada frente a algunos tipos de amenazas. Finalmente, se presenta un análisis económico que revela el ahorro que puede suponer la adopción de la solución propuesta frente a otras alternativas.

4.1. Requisitos generales y consideraciones del sistema

Para probar la usabilidad real del modelo propuesto y su integración en un sistema de trazabilidad con control de calidad, se ha integrado el sistema descrito en el punto anterior en un prototipo de sistema de trazabilidad basado en RFID. Esto ha permitido verificar su fiabilidad, eficiencia y comprobar que los tiempos de procesado de firmas son compatibles con los tiempos de producción real, ya que, al tratarse de una cadena manufacturera, en cada uno de los puntos de control hay un tiempo limitado para realizar las verificaciones, incorporar los atributos a la identidad y almacenarla en el sistema (tanto en el soporte físico de almacenamiento como en el sistema de información).

Se ha desarrollado un prototipo en uno de los elementos intermedios de una cadena de suministro de un producto cárnico elaborado, concretamente para un matadero del Consejo Regulador de la Denominación de Origen (CRDO) del Jamón de Teruel.

Al tratarse de un producto alimenticio, se debe valorar y analizar una serie de parámetros regulados por leyes, tanto nacionales como europeas, sobre el control de alimentos (ver apartado 4.1.1). Además, al ser un producto amparado por una Denominación de Origen Protegida, se deberán cumplir una serie de requisitos que se detallan en el pliego de condiciones el Consejo Regulador correspondiente (ver apartado 4.1.1) para poder marcar los productos finales como pertenecientes a dicha Denominación de Origen.

La elección de este producto para realizar las pruebas del sistema de trazabilidad responde a la posibilidad de obtener una serie de datos que con otro tipo de productos no sería posible. La característica principal que aporta esta elección, es la de trabajar con un producto con un volumen de negocio

importante. Según los datos publicados por la Subdirección General de Calidad Diferenciada y Agricultura Ecológica del Ministerio de Medio Ambiente y Medio Rural y Marino, en el informe "Datos de las Denominaciones de Origen Protegidas (D.O.P.) e Indicaciones Geográficas Protegidas (I.G.P.) de Productos Agroalimentarios[18]" de 2010, en el citado año se produjeron 525.328 jamones bajo esta denominación, lo que supuso un volumen de unos 37'82 millones de euros.

4.1.1. Salud pública y legislación

Antes de comenzar con los aspectos más técnicos, se va a exponer un breve resumen del conjunto de normas que se deben contemplar al realizar la trazabilidad de un alimento. La legislación vigente regula tanto el apartado de trazabilidad como el de salud pública.

El Reglamento Europeo Nº 178/2002 (Regulation (EC) 178/2002) establece los principios y requisitos generales de la legislación alimentaria y fija los procedimientos relativos a la seguridad alimentaria. Esta norma podría considerarse la fundamental, a partir de la cual fueron surgiendo todas las demás. En sus consideraciones iniciales, apartados 28 y 29, y más desarrollada en el artículo 18, indica que es necesario establecer un sistema de trazabilidad en las empresas alimentarias. Otro punto importante se encuentra en las consideraciones iniciales, apartado 30, y también en el artículo 19. Éste indica que el responsable legal de la seguridad alimentaria es el explotador de la empresa alimentaria.

También se tendrán que cumplir los requisitos que impone el Consejo Regulador, que se han ido adaptando a la realidad desde su primera versión[19] de 1993, ligeramente modificada[20] en 2005, adaptada[21] en 2009, y finalmente nuevamente revisada[22] *y* [23] en el año 2012. Estos requisitos siempre serán un añadido a los ya establecidos por la normativa española y europea. Las principales

[18] *Últimos datos disponibles, a la fecha de cierre de esta memoria de tesis.*

[19] *ORDEN, de 3 de Noviembre de 1993, por la que se ratifica el l Reglamento de la Denominación de Origen «Jamón de Teruel» y su Consejo Regulador.*

[20] *ORDEN de 18 de febrero de 2005, por la que se modifica el Reglamento de la denominación de Origen «Jamón de Teruel» y de su Consejo Regulador, aprobado por la Orden de 29 de julio de 1993. Y ORDEN APA/1235/2005, de 22 de abril, por la que se ratifica la modificación del Reglamento de la Denominación de Origen «Jamón de Teruel».*

[21] *ORDEN de 6 de febrero de 2009, del Consejero de Agricultura y Alimentación, por la que se aprueba la normativa específica de la denominación de origen protegida "Jamón de Teruel", incluye, como anexos, el pliego de condiciones, el reglamento de funcionamiento y los estatutos.*

[22] *ORDEN de 28 de junio de 2011, del Consejero de Agricultura y Alimentación, por la que se adopta la decisión favorable en relación con la solicitud de modificación del pliego de condiciones de la Denominación de Origen Protegida Jamón de Teruel*

[23] *ORDEN de 2 de marzo de 2012, del Consejero de Agricultura, Ganadería y Medio Ambiente, se han resuelto los recursos de reposición interpuestos contra la Orden de 28 de junio de 2011, del Consejero de Agricultura y Alimentación, por la que se adopta la decisión favorable en relación con la solicitud de modificación del pliego de condiciones de la denominación de origen protegida "Jamón de Teruel".*

restricciones impuestas por la DO son de tipo geográfico (tanto las granjas, como los cebaderos y secaderos deberán ubicarse en municipios de la provincia de Teruel y en el caso de los secaderos con una altitud media no inferior a 800 metros), así como otras referentes a la procedencia, producción y calidad del jamón (como es el tipo de raza del animal, peso mínimo y máximo o el tiempo de maduración y curación de los jamones, controles de calidad, etc.). Al final de este apartado se reflejan las principales características que debe cumplir el producto según el pliego de condiciones del Consejo Regulador.

Respecto a la trazabilidad y la seguridad alimentaria, a continuación se presenta un resumen de normativa[24] recogida en [AESAN2009], y que afecta a estos ámbitos:

- **Reglamento (CE) Nº 178/2002** del Parlamento Europeo y del Consejo de 28 de enero de 2002 por el que se establecen los principios y los requisitos generales de la legislación alimentaria, se crea la Autoridad Europea de Seguridad Alimentaria y se fijan procedimientos relativos a la seguridad alimentaria (D.O.C.E: nº L31 de 1.2.2002). El **artículo 18** de la citada disposición establece por primera vez, con carácter horizontal, para todas las empresas alimentarias y de piensos que forman parte de la cadena alimentaría la obligación de poner en marcha, aplicar y mantener un sistema de trazabilidad. Dicho artículo es aplicable desde el 1 de enero de 2005. **El artículo 19** establece las responsabilidades respecto a los alimentos de los operadores económicos cuando se detecte que algún alimento no cumple los requisitos de seguridad. También se establece la obligación por parte del operador de la retirada del producto. El **artículo 20** dispone las mismas responsabilidades para el operador económico de empresa de piensos.
- **Libro Blanco sobre la Seguridad alimentaria.** La Comisión Europea perfiló una revisión radical de las normas de higiene y seguridad alimentaria de la Comunidad, conforme a las cuales, los operadores de empresa alimentaria son los principales responsables de la seguridad alimentaria. La innovación principal, es la realización de una política de higiene única, transparente y aplicable a todos los alimentos y todos los operadores de alimentos que intervienen de la granja a la mesa, junto con la introducción de instrumentos eficaces

[24] *En el Anexo IV se amplía esta información.*

para gestionar la seguridad alimentaria y cualquier crisis alimentaria en todas las etapas de la cadena de alimentos.

- **Reglamento (CE) Nº 852/2004** del Parlamento europeo y del Consejo de 29 de abril de 2004 relativo a la higiene de los productos alimenticios (H1) (D.O.C.E: nº L 226 de 25.6.2004). En el **artículo 5** se establece la obligación para los operadores de empresa alimentaria que intervengan en cualquier etapa de la producción, transformación y distribución de alimentos posteriores a la producción primaria de crear, aplicar y mantener un procedimiento o procedimientos permanentes basados en los principios del APPCC (Análisis de Peligros y Puntos Críticos de Control). Dicho sistema implica la elaboración de documentos y registros en función de la naturaleza y el tamaño de la empresa alimentaria para demostrar su aplicación efectiva, que pueden contribuir a la información necesaria del sistema de trazabilidad.
- **Reglamento (CE) Nº 853/2004** del Parlamento europeo y del Consejo de 29 de abril de 2004 por el que se establecen normas específicas de higiene de los alimentos de origen animal (H2) (D.O.C.E. nº L 226 de 25.6.2004). Los operadores de empresa alimentaria responsables de los establecimientos sujetos a autorización con arreglo al presente Reglamento deben asegurarse de que todos los productos de origen animal que pongan en el mercado llevan una marca sanitaria o una marca de identificación.
- **Reglamento (CE) Nº 183/2005** del Parlamento europeo y del Consejo de 12 de enero de 2005 por el que se fijan requisitos en materia de higiene de los piensos (D.O.C.E. L 35 de 8.2.2005). El **artículo 6** fija los requisitos en materia de higiene de los piensos.
- **Real Decreto 1808/1991,** de 13 de diciembre, que regula las menciones o marcas que permiten identificar el lote al que pertenece un producto alimenticio (BOE 25.12.1991). Resultado de la transposición de la Directiva del Consejo 89/396/CEE, de 14 de junio de 1989, esta legislación requiere una indicación o marca de identificación del lote al que pertenece el alimento.

Además de las normas citadas, basadas en la información contenida en [AESAN2009], para el caso que nos ocupa, existe legislación propia de la comunidad autónoma donde se lleva a cabo la actividad de producción, en este caso Aragón, y que se cita a continuación:

- **Ley 9/2006, de 30 de noviembre, de Calidad Alimentaria en Aragón** ("Boletín Oficial de Aragón" Nº 142, de 13 de diciembre de 2006).
- **Decreto 5/2009, de 13 de enero, del Gobierno de Aragón**, por el que se aprueba el Reglamento del contenido mínimo de la normativa específica de determinadas denominaciones geográficas de calidad de los alimentos y el procedimiento para su reconocimiento ("Boletín Oficial de Aragón" Nº 18, de 28 de enero de 2009).

Como se ha comentado anteriormente, además de esta legislación de carácter general, en el caso del Jamón de Teruel debe contemplarse también el pliego de condiciones de la propio Consejo Regulador de la Denominación de Origen Jamón de Teruel (Orden de 28 de junio de 2011, del Boletín Oficial de Aragón), y en el que se recogen las características que debe tener el producto en cada una de sus etapas de producción. Para el presente trabajo son importantes, ya que todas ellas deben ser verificadas y por tanto son susceptibles de ser incorporadas a la identidad del producto avaladas por una firma digital. A continuación, se presentan estos requisitos:

- **Requisitos relativos a los lechones, piensos y cerdos** ("Granja y cebadero"):
  - *Los jamones y paletas curadas procederán exclusivamente de las razas Landrace (tipo estándar), Large White o cruce de ambas (línea madre), y Duroc (línea padre).*
  - *Tanto las granjas de producción de lechones como las granjas de cebo de cerdos estarán inscritas y situadas dentro de la zona de producción.*
  - *Los machos estarán castrados antes de la entrada en el cebadero.*
  - *Los animales estarán identificados, a su entrada en cebaderos, por una marca indeleble en la oreja, en la que figurará el código de explotación de la que proceden.*
  - *Los elaboradores de piensos compuestos para la alimentación de los cerdos amparados por la Denominación de Origen Protegida, deberán estar ubicados dentro del área geográfica de la provincia de Teruel.*
  - *La alimentación del ganado se basa fundamentalmente en cereales, definiendo los porcentajes de materias primas que entran a formar parte de la composición del pienso, que se formulará con un mínimo de 50 % de cereales. Las fábricas de pienso deberán justificar que al menos el 20 % de los cereales utilizados en la fabricación del pienso en un año proceden de los cultivos de la propia provincia de Teruel.*

- ***Requisitos relativos al sacrificio*** *("Matadero"):*
    - *El transporte, sacrificio, curación (secado y maduración) y envejecimiento de los perniles y paletas estarán controlados por el Consejo Regulador.*
    - *El ganado será transportado en camiones con montacargas, o vehículos adecuados, de forma que los cerdos no sufran ninguna alteración o molestia que pueda afectar a su estado o integridad física.*
    - *El sacrificio de los cerdos destinados a la obtención de perniles y paletas que optan a la Denominación de Origen se realizará en mataderos inscritos dentro de la zona de producción.*
    - *Las hembras no estarán en celo en el momento del sacrificio.*
    - *Los cerdos guardarán ayuno un mínimo de 12 horas antes de sacrificio.*
    - *Los mataderos deberán reunir las condiciones técnico-sanitarias exigidas en la legislación vigente y en ellos permanecerá el cerdo, antes de su sacrificio, un tiempo de espera con el fin de eliminar la fatiga del transporte y asegurar un nivel mínimo de las reservas del glucógeno muscular. Durante este tiempo se les proporcionará a los animales agua "ad libitum".*
    - *El sacrificio del animal se realizará con aturdimiento previo, mediante todos aquellos métodos oficialmente reconocidos, además del electro-shock. Se exigirá posteriormente, el más completo desangrado y no se podrá taladrar las extremidades posteriores y anteriores del cerdo.*
    - *Únicamente podrán suministrar piezas con destino a la elaboración de jamones y paletas curadas protegidas por la Denominación de Origen, las canales de cerdos cuyos pesos en caliente sean superiores o iguales a 86 kg. y cuyo espesor de tocino dorsal, medido en la zona lumbar a la altura de la punta del pernil, sea superior a 16 milímetros e inferior a 45 milímetros.*
    - *Una vez despiezada la canal y perfilados los perniles y paletas, se mantendrán a una temperatura entre –2ºC y +2ºC, el tiempo necesario para conseguir una temperatura máxima de +2ºC en el interior de la pieza. El transporte de los perniles y de las paletas desde el matadero a los locales de curación se hará en vehículos frigoríficos, entrando en la nave de salado con una temperatura en el centro del pernil y de la paleta entre 0 y 2ºC.*

- ***Requisitos relativos a la elaboración y maduración*** *("Secadero"):*
    - *Los secaderos en los que se efectúen las fases de curación y envejecimiento del jamón y de la paleta se realizarán en locales inscritos, ubicados en la zona de elaboración y controlados por el Consejo Regulador. Los envasadores*

igualmente estarán inscritos y ubicados dentro de la zona de elaboración, en locales inscritos y controlados por el Consejo Regulador.

- *Proceso de elaboración: a partir de este momento se procede al proceso de elaboración, que consta de cinco operaciones: Salazón, lavado, post-salado, curado (secado-maduración) y envejecimiento:*
  - ***Salazón**: es la incorporación de sales a la masa muscular, que favorecen la deshidratación de las extremidades del cerdo y su perfecta conservación. La sal permanece en contacto con las piezas entre 0.65 y 1 día por Kilogramo de peso fresco de pernil o de paleta.*
  - ***Lavado**: se lavan con agua para eliminar la sal adherida.*
  - ***Asentamiento o postsalado**: en esta fase se produce la difusión de la sal hacia el interior de todas las piezas cárnicas, eliminándose lenta y paulatinamente el agua. El proceso se realiza en cámaras con temperaturas máximas de 6 ºC y una humedad relativa igual o mayor del 70%. El tiempo de permanencia en las cámaras depende del peso de las piezas, teniendo que ser este un mínimo de 60 días para los jamones y de 30 días para las paletas.*
  - ***Curado** (secado y maduración): esta operación se lleva a cabo en secaderos cuyas condiciones ambientales son las propias de la zona, controlando la ventilación para conseguir las condiciones óptimas de humedad relativa y temperatura.*
  - ***Envejecimiento**: En esta fase se producen las reacciones bioquímicas responsables del aroma y sabor característico.*
- *La duración mínima de todo el proceso de elaboración es de 60 semanas para los jamones y de 36 semanas para las paletas.*
- *Finalizado todo el proceso citado anteriormente, los jamones y paletas en piezas enteras salen al mercado con la garantía de su origen, materializada en la palabra "TERUEL" con la estrella de 8 puntas marcada a fuego y la contraetiqueta (vitola) numerada por el Consejo Regulador.*

Como se puede apreciar, todo el proceso con sus diferentes características y condiciones está perfectamente definido, por tanto es susceptible de verificarse y añadirse a la etiqueta que almacena la identidad digital del producto.

4.1.2. Tratamiento de la información y puntos de control

La cadena de suministro del Jamón de Teruel involucra la totalidad de la vida del producto: granja de nacimiento de los lechones, alimentación, obtención de los perniles y las fases de curación y maduración. Como se representa en la Fig. 4-1.

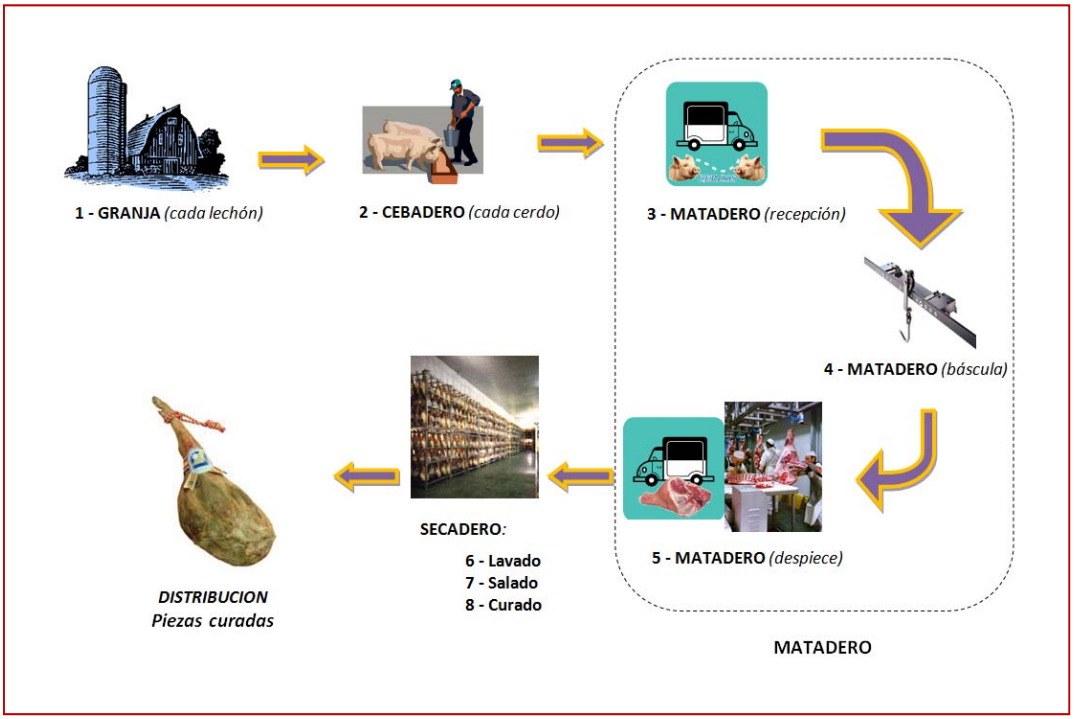

Fig. 4-1. Esquema del proceso productivo.

El escenario en el que se va a implantar el prototipo del sistema de trazabilidad es un matadero del CRDO del Jamón de Teruel, encargado de la obtención de los perniles (la parte rodeada por una línea de puntos en la Fig. 4-1).

El sistema de trazabilidad se basa en unos puntos de control o *checkpoints* que se ajustan a los requisitos descritos en el apartado anterior. En el matadero, que es la parte del proceso para la que se ha desarrollado el prototipo, se han establecido cuatro puntos de control o *checkpoints,* que son los siguientes:

- **Entrada/Recepción de los animales (lotes)**: el terminal de introducción de datos suele ubicarse en las oficinas, aunque

también se puede ubicar en los corrales o en el puesto del veedor[25]. Antes de iniciar la jornada de sacrificio, para poder realizar la trazabilidad en tiempo real, se introducen los datos de los lotes que se sacrificarán en esa jornada.

- **Control de canales (veedor):** a este punto llegan los animales sacrificados, eviscerados y colgados de unas perchas para el pesado de las canales. Desde la base de datos se cargan los datos de los lotes del día actual (número de lote activo, número de guía sanitaria y corrales) y de la explotación ganadera de origen (nombre y códigos REGA[26] y CRDO). De forma similar a la mostrada en la Fig. 4-2, se comprueba el peso de la canal, el espesor de tocino, que no haya algún defecto, el sexo y se genera el rol de sacrificio. Este rol, definido por el CRDO, es un número de 10 dígitos que deberá ser visible sobre los perniles. Este número incluye un dígito que identifica al matadero, dos que informan sobre la semana de sacrificio, tres para identificar la explotación de origen y un número creciente (4 dígitos) que cuenta los animales de la misma granja sacrificados esa misma semana. Es decir, hay una cuenta por granja y semana. Además de esta información, en la identidad también se integran otros atributos como la identificación del agente de control, el número de identificación único *(UID)* de la etiqueta RFID, la fecha y la hora. Toda esta información es avalada por la firma digital electrónica del agente de control.

Fig. 4-2. Control de canales por parte del veedor.

[25] *Agente de control encargado de realizar las verificaciones de las características de las canales.*
[26] *Registro general de explotaciones ganaderas.*

- **Control de perniles**: Tras el despiece, a este punto (ver Fig. 4-3) llegan los perniles limpios y perfilados tras un proceso de manipulación y selección de las piezas por parte de los operarios. Un agente de control es el encargado de llevar a cabo las labores de verificación de las características de los jamones de Teruel con Denominación de Origen (verifica que el peso sea adecuado, la jaula en la que se va a colgar cada pernil y la ausencia de taras). Se comprueba la validez de la firma anterior, y se añaden los nuevos atributos, junto con la identificación del agente de control, la fecha y la hora, generándose una nueva firma agregada. El terminal para la introducción de datos debe estar situado junto a la balanza de pesaje de los perniles, que usualmente estará directamente conectada a él.

Fig. 4-3. Punto de control de perniles.

- **Expedición:** El último puesto se sitúa a la salida del matadero en el punto desde donde se expiden los perniles hacia los secaderos. Como se muestra en la Fig. 4-4. los perniles se colocan provisionalmente en jaulas a la espera de ser colgados en espadas, jaulas, o cajas. El único dato que queda por incorporar a la identidad del producto es el secadero de destino y la fecha de salida de los perniles del matadero. El proceso en este punto del sistema es muy dependiente de método de trabajo y almacenamiento de perniles de cada instalación.

Fig. 4-4. Jaula de expedición

4.1.3. Escenario físico

Una de las claves de la implantación exitosa de la tecnología RFID es la selección adecuada de la etiqueta RFID y el sistema de colocación, ya que debe ser colocada en una cadena de producción y por tanto el tiempo para colocarla es limitado.

Dadas las condiciones de elevada humedad, bajas temperaturas y presencia de superficies metálicas, se estimó [LÓPEZ2009] que lo más adecuado era el uso de etiquetas que operaran en la banda de trabajo de 13'56 MHz [Auto-ID Center2003a].

Las etiquetas que han sido utilizadas son las NXP I-code SLI que tienen una memoria de 1024 bits. Además, la etiqueta no debe afectar a la calidad de la carne, por lo que deben utilizarse o bien adhesivos cárnicos o bien otros sistemas de sujeción mecánica. Como primera opción se utilizó un adhesivo cárnico SD2800 que cumplía la regulación (EC) Nº 1935/2004, y se podía utilizar con la impresora disponible, pero en las pruebas en el matadero se pudo comprobar que más del 50 % de las etiquetas fallaban y se despegaban, probablemente debido a la alta temperatura a la que se somete a la carne en algunos puntos del proceso así como a las tareas de lavado. Tras el estudio del problema, y la consideración de diversas alternativas, se decidió que la solución más razonable era fijar las etiquetas mediante el uso de bridas y navetes.

Para el punto de control de canales, se utilizó una impresora RFID Avery Denninson Monarch 9855que opera en la banda de Alta Frecuencia (HF, 13'56

MHz). Tras diferentes pruebas del prototipo se comprobó el correcto funcionamiento y que siempre se escribían los datos en posiciones fijas. Adicionalmente a la información que se almacena en la memoria de la etiqueta, simultáneamente también se imprime en la superficie un número denominado "rol", procedente del anterior sistema de trazabilidad, y que permite la identificación visual de las piezas. El uso de este sistema de información redundante, minimiza los riesgos de pérdidas de información o productividad por fallos en el sistema de identificación electrónica, lo que también ayuda en la fase de implantación a minimizar las reticencias de los usuarios.

En la Tabla 4-1, se muestran los datos almacenados en la memoria interna de la etiqueta RFID, una vez se ha completado el proceso.

DATOS	Tamaño (Bytes)
Firma agregada	21
Código CRDO cebadero	2
Peso Canal	2
Núm. Rol Sacrificio	2
Identificación Matadero	1
Fecha + Hora sacrificio	4
Identificación veedor	1
Peso pernil	2
Jaula asignada	1
Fecha + Hora despiece	4
Id. operario despiece	1

Tabla 4-1. Datos etiqueta RFID

La memoria de la etiqueta está estructurada en 20 bloques de 4 bytes (ver Fig. 4-5). Cada vez que se desea grabar un dato en una posición determinada, es necesario recorrer todos los bytes anteriores (empezando por el 0), para llegar a él. Dado que la firma agregada es el campo de mayor tamaño y debe ser leído y escrito varias veces, se decidió asignar a este parámetro los bytes a los que se accede en primer lugar.

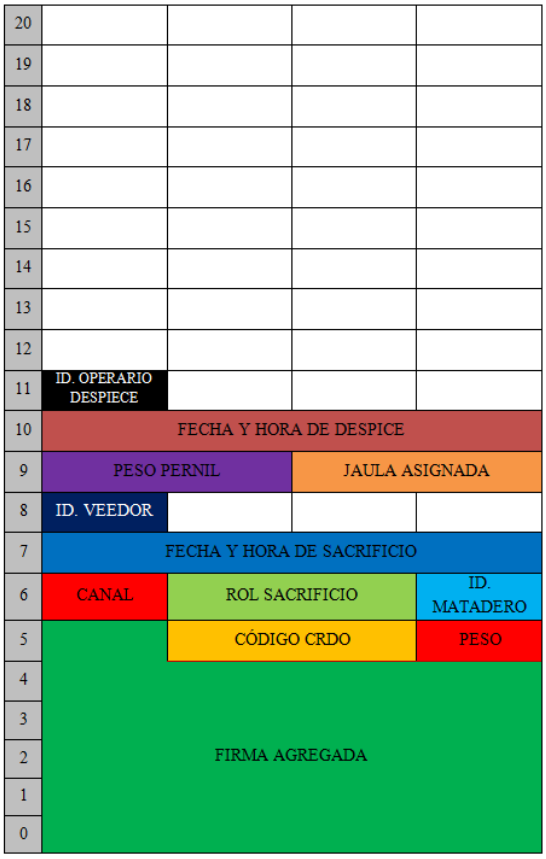

Fig. 4-5. Distribución memoria etiqueta RFID

Como se puede observar, la etiqueta tiene espacio para incluir futuros procesos, además dado que el tamaño de la firma agregada se mantiene constante, el sistema es muy escalable.

Para su construcción, descrita en [LÓPEZ2009], se han utilizado lectores RFID de alta frecuencia, PCs y una red de comunicaciones que conecta cada uno de los PCs asociados a cada lector con la base de datos. La distancia de trabajo entre cada lector y su PC es de 1 metro.

El sistema de flujo de comunicaciones que se decidió implementar en el prototipo fue un sistema centralizado. Se instaló en cada *checkpoint* un lector/grabador RFID y un terminal. Se utilizó una red cableada basada en Ethernet para realizar las conexiones necesarias entre los terminales y el servidor central, en el que se desarrollan las operaciones de firma y verificación. De esta manera se redujeron los costes relacionados a los terminales y dado que el número de puntos de control no es muy elevado, los requisitos del servidor central tampoco son muy altos. Además, en beneficio de la seguridad, el servidor de firmas es distinto del servidor donde se aloja la base de datos. El esquema puede verse en la Fig. 3-5, en el capítulo 3.

4.2. Requisitos específicos de seguridad

La seguridad a nivel general en el ámbito RFID se centra en cuatro grandes campos:

1. Mantener la privacidad y evitar la trazabilidad.
2. Proteger los datos que hay en las tarjetas.
3. Autenticación entre lectores y tarjetas.
4. Garantizar la autenticidad e integridad de los datos.

Tras la revisión bibliográfica, se observa que las necesidades de seguridad para este prototipo tienen una casuística particular, diferente de los objetivos de la gran mayoría de los casos presentados en la literatura revisada.

Tras el estudio de las necesidades, ver apartado 4.1, se detectaron una serie de condiciones de contorno referentes a la seguridad del prototipo, que se resumen a continuación:

1. No se necesita mantener la privacidad, ya que todo el trabajo se realiza en una cadena de producción dentro de un matadero y no hay datos secretos.
2. La trazabilidad no es algo a evitar sino el objetivo del proyecto, por tanto no hay que preocuparse por este aspecto (es una de las líneas que mayores recursos materiales y humanos acapara actualmente dentro de la seguridad RFID).
3. No es necesaria una autenticación de los dispositivos de lectura/grabación de etiquetas RFID, ya que la seguridad se aporta en los propios datos que se grabarán en la etiqueta.
4. Se debe garantizar que los datos sean avalados por agentes autorizados y que se responsabilizan de la veracidad de los datos que firman (autenticidad).
5. Se debe poder detectar si los datos han sido alterados (integridad).

El modelo de identidad digital certificada basada en firmas agregadas planteado en esta tesis supone una solución sencilla y económica en este tipo de sistemas con este perfil de requisitos de seguridad, ya que las operaciones

criptográficas pueden ser realizadas por los ordenadores que siempre están asociados a los lectores y por tanto las etiquetas se convierten en meros soportes de información. Con este planteamiento el problema del mínimo coste de las tarjetas queda salvado.

El segundo problema que debe resolverse, también inherente al coste de las tarjetas, es la importante limitación de memoria de la tarjeta que en el mejor de los casos es de 1 KB. De este tamaño máximo se deben sustraer los bits ocupados por la información fija que debe haber en la tarjeta, así como los datos que se van incorporando durante el proceso.

Si se planteara esta solución basada en un sistema de infraestructura de clave pública tradicional concatenando firmas, sería necesaria una gran cantidad de memoria para guardar la identidad de los firmantes y las firmas. Para hacerse una idea, podemos suponer que si el sistema tuviera 4 puntos de control, y tomando los 320 bits que proporciona DSA trabajando con módulos de 1024 bits, tendríamos ocupado un espacio de 1280 bits sólo con las firmas, lo que desbordaría la capacidad de la tarjeta.

Para resolver este problema, minimizar el espacio de memoria ocupado, se llegó a la conclusión que una solución podría ser el uso de firmas agregadas en el proceso.

4.3. Elección del tipo de curva elíptica y tamaño de clave.

Como se debe alcanzar un compromiso entre el nivel de seguridad requerido y el tamaño de la firma, la solución elegida está basada en el esquema propuesto por Boneh en [BONEH2004].

En cada uno de los puntos de control, tras verificar la firma se procederá a agregar el mensaje correspondiente a ese punto y la nueva firma agregada. Por ejemplo, en el punto de control tres el mensaje a escribir sería:

$$\{d\{d'\{d''\}\}\}FA_{ABC} \qquad (4\text{-}1)$$

donde *d* representa los datos incluidos en el primer mensaje, *d'* los del segundo y *d''* los del tercero. FA significa firma agregada, en este caso FA_{ABC} representa la firma agregada de los firmantes A (mensaje *d*), B (mensaje *d'*) y C (mensaje *d''*).

Los datos *d* estarán compuestos por la información que se deba incorporar en cada punto más la hora y la fecha en la que se realice la incorporación, lo que

además garantizará que cada uno de los mensajes firmados sea distinto de los demás, que es un requisito impuesto por el tipo de firma utilizado.

También como paso previo a la introducción de nuevos datos y a su correspondiente nueva agregación de firma, se verificará que hasta ese punto la firma es correcta. En caso de que la comprobación la detecte como errónea, no se producirá la firma de ese punto.

En el apartado siguiente, se resume el estudio que se hizo de las diferentes alternativas respecto al tiempo de procesado, para seleccionar el tipo de curva y el tamaño de la clave.

4.3.1. Tiempo de procesado

Una de las ventajas del uso de este modelo en un sistema de trazabilidad radica en que el tiempo de procesado y verificación de firma es muy rápido, y por tanto es difícil que supere el tiempo utilizado por la cadena de procesado en ninguno de los puntos de control.

Antes de seleccionar el tipo de curva y el tamaño de la clave, se realizaron pruebas para ver el rendimiento, concretamente el tiempo de procesado para distintas curvas, distintas longitudes de firma y distinto número de firmantes.

4.3.1.1. Primera batería de pruebas.

El banco de pruebas utilizado para la realización de los cálculos criptográficos fue un PC estándar sin ninguna característica especial (procesador AMD Athlon64 3500+ con 2Gb de RAM). Para las primeras pruebas de integración con el sistema de RFID se utilizó un lector-grabador, ubicado en un laboratorio, que funcionaba en la banda de 13.56 MHz, capaz de interactuar con transpondedores basados en los estándares ISO 14.443 (partes 2, 3 y 4) e ISO 15.693. El dispositivo también soportaba algoritmos estándar de cifrado (DES, 3DES y AES), funciones de hash (SHA y MD5), y poseía un generador interno de números pseudo-aleatorios (PRNG).

Se realizaron pruebas con curvas y tamaños de firma diferentes, evaluando también el tiempo de procesado de cada una, obteniendo los siguientes resultados (Tabla 4-2):

Nº Firmas	160 bits No-SS	256 bits No-SS	307 bits No-SS	127 bits SS	255 bits SS	511 bits SS	767 bits SS	1023 bits SS
2	0,5	0,96	1,33	0,05	0,15	0,36	0,75	1,23
3	0,66	1,29	1,8	0,07	0,19	0,49	0,99	1,65
4	0,82	1,61	2,24	0,09	0,24	0,62	1,26	2,05
5	0,99	1,98	2,7	0,11	0,29	0,74	1,5	2,47
6	1,15	2,32	3,19	0,13	0,34	0,86	1,75	2,88
7	1,35	2,6	3,59	0,15	0,39	0,99	1,99	3,33
8	1,49	2,95	4,07	0,17	0,44	1,11	2,25	3,77

Tabla 4-2. Tiempo en seg. de procesado de firma agregada. SS: Curva Supersingular. No-SS: Curva no súper singular

Es importante señalar, que dado que el tiempo de generación de la firma es muy pequeño en comparación con el tiempo de verificación, se puede tomar como tiempo de procesado de la firma (tiempo de verificación + tiempo de generación de la firma) el tiempo de verificación.

A continuación, en la Fig. 4-6, se puede apreciar el tiempo de procesado para la verificación de la firma agregada dependiendo de la cantidad de firmantes implicados. Se puede concluir que son prácticamente lineales ya que la verificación implica la ejecución de un emparejado bilineal por cada firmante. Las curvas empleadas pertenecen a 2 familias: las supersingulares (SS) y las no supersingulares (no-SS).

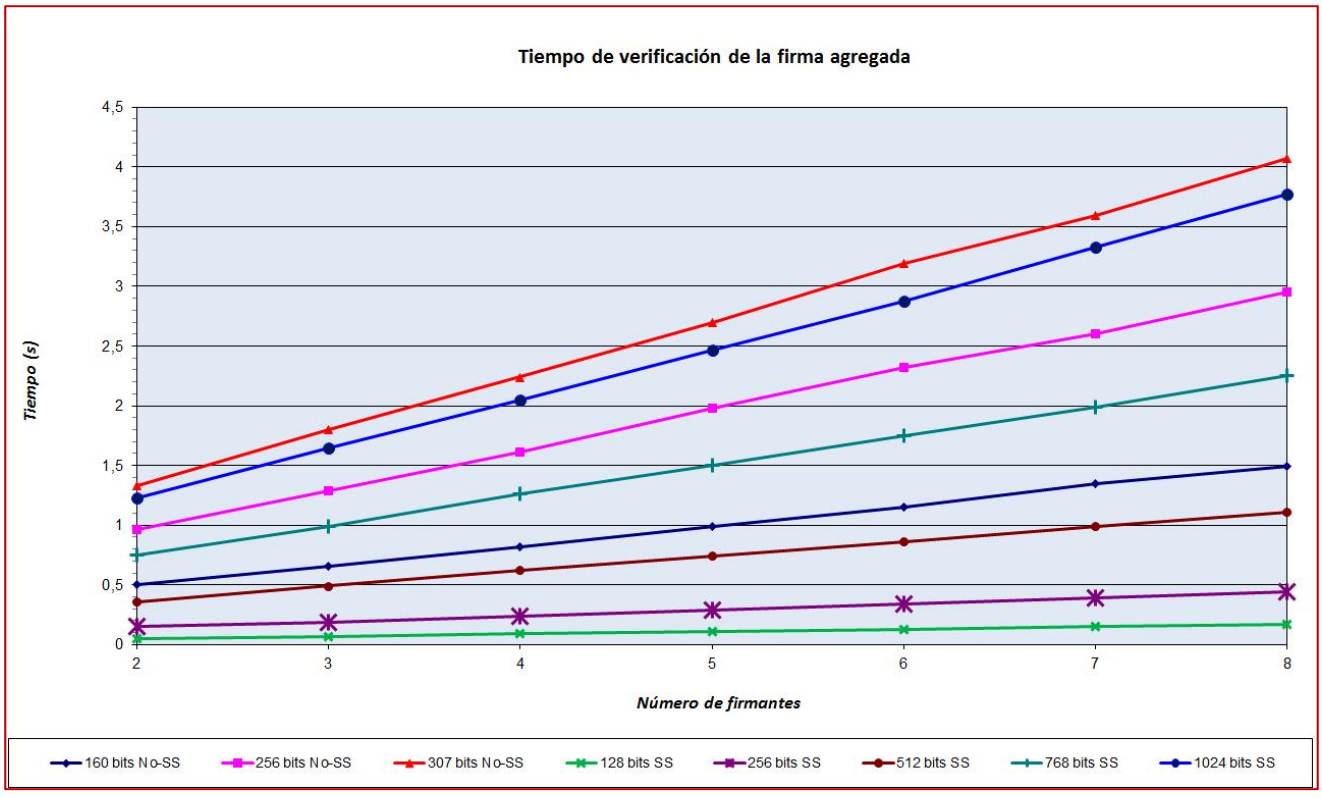

Fig. 4-6. Comparación de tiempo de verificación de firma de distintos tipos de curva y tamaños de firma

A la vista de los resultados, para cada situación, se elegirá la tipología de curva conforme a las variables de potencia de procesado disponible y de nivel de seguridad que se deba proporcionar, según determine el equipamiento disponible y el entorno de aplicación.

Por su parte en las figuras Fig. 4-7 y Fig. 4-8, se pueden comparar también los tiempos de procesado para las dos tipologías de curvas (supersingulares y no supersingulares).

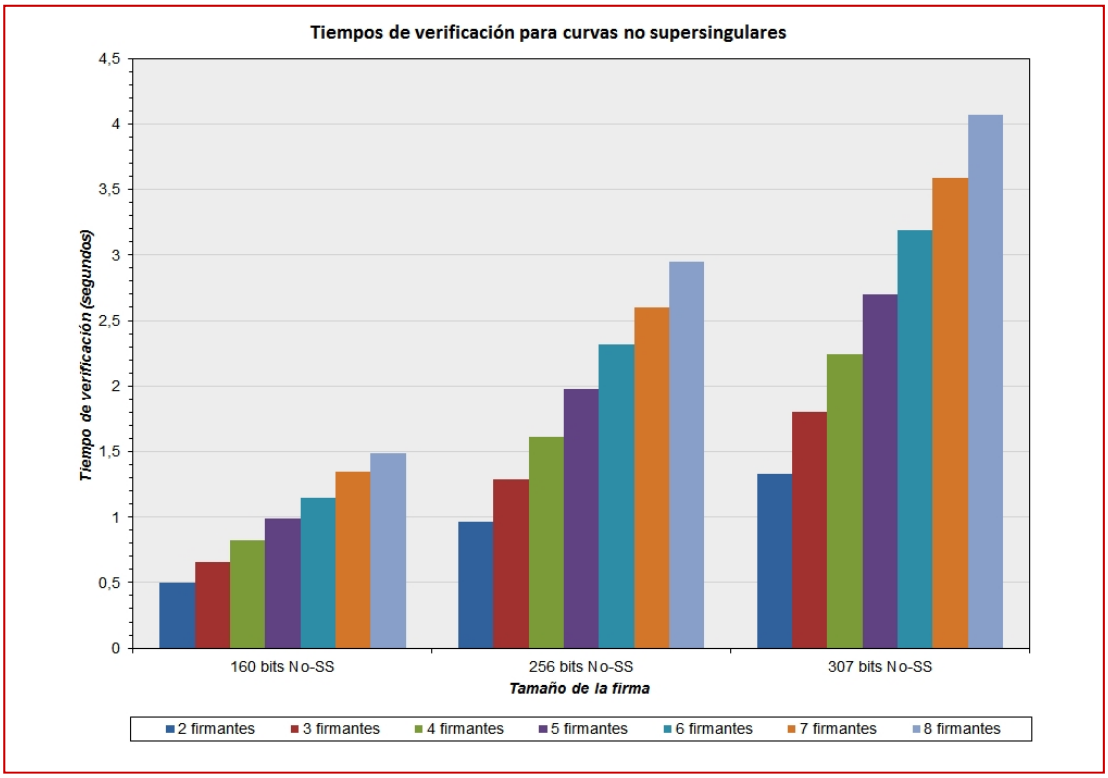

Fig. 4-7 Tiempo de procesado de firmas No supersingulares – comparativa por longitud de clave

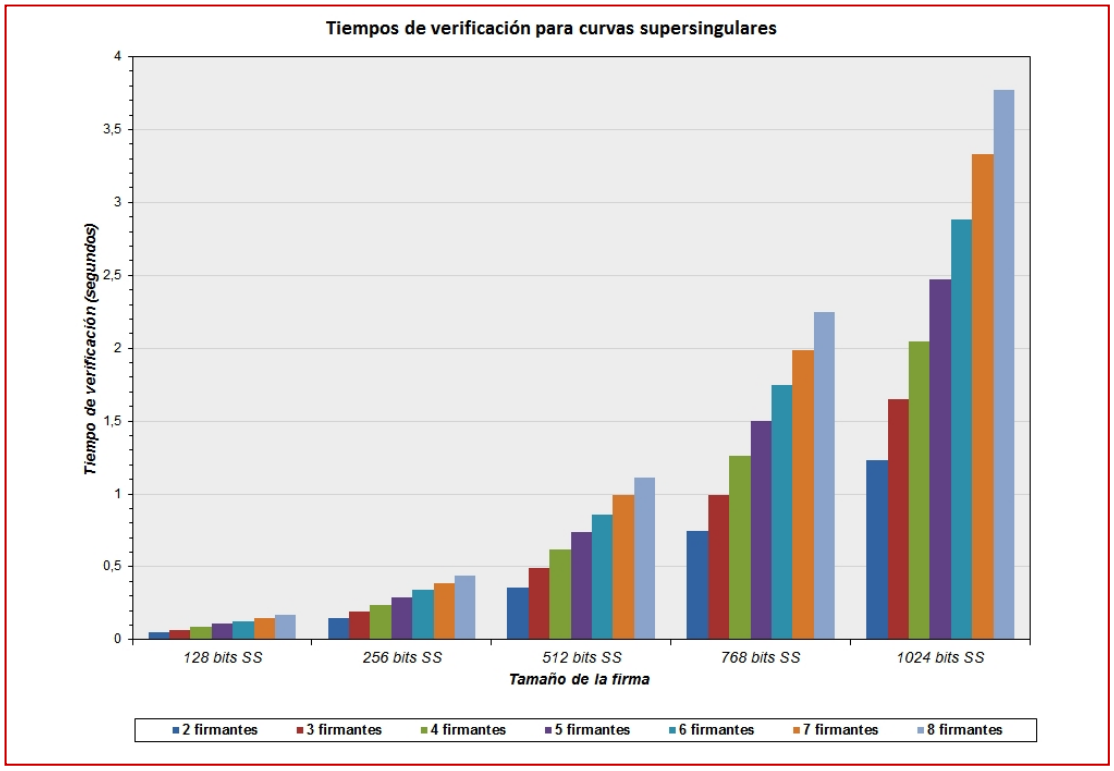

Fig. 4-8 Tiempo de procesado de firmas Supersingulares – comparativa por longitud de clave

En las figuras anteriores se aprecia claramente que el tiempo de procesado de las curvas no-supersingulares es en niveles cuantitativos mucho mayor. No obstante, debido a que el nivel de seguridad que ofrece cada una de las curvas viene determinado por la longitud de sus claves multiplicada por el factor MOV de la curva, que es de 2 en las curvas supersingulares y de 6 en las no supersingulares, vamos a comparar ahora las curvas fijando un nivel similar de seguridad. Tomemos un tamaño de firma de 160 bits en la curva no-SS, que multiplicado por el factor MOV=6, obtenemos un nivel de seguridad equivalente de 960. Para un nivel similar de seguridad equivalente, tomaremos las firma de 512 bits en la curva supersingular (MOV=2), lo que nos dará un nivel de seguridad equivalente de 1024, del orden del anterior. También hay que añadir que la elección del grado MOV igual a 6 viene determinada porque es el nivel máximo en el que este tipo de curvas es operativo. Con valores más altos de 6, las operaciones implicadas en el cálculo de emparejados bilineales alcanzan una complejidad excesiva. La comparación se muestra gráficamente en la Fig. 4-9.

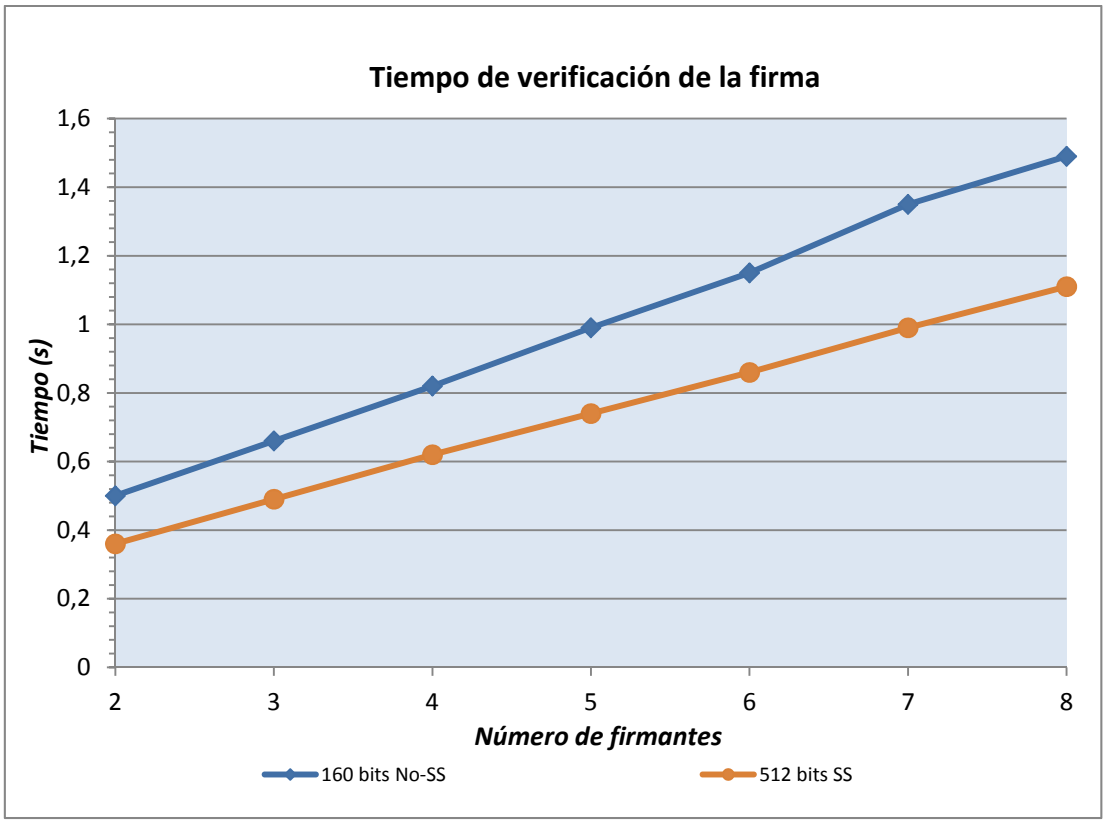

Fig. 4-9. Comparación de tiempos de verificación entre curvas y tamaños de firma con nivel de seguridad equivalente similar

Como se puede apreciar en la Fig. 4-9, el tiempo es prácticamente similar (en torno a un 35 % más corto en la SS), pero en los valores de tiempo que nos movemos no es un factor determinante, ya que ambos cumplen con los requisitos de tiempo impuestos por la cadena de producción. Para realizar la elección, nos centraremos en las fuertes restricciones de memoria que impone el uso de las tarjetas RFID de ultra-bajo coste utilizadas, y por tanto se elegirá la curva no supersingular por ofrecer un importante ahorro en el espacio de memoria ocupado por la firma (casi un 70 % de ahorro).

A la vista de todo lo anterior, se concluye elegir un tamaño de firma de 160 bits y la curva no-supersingular.

4.3.1.2. Segunda batería de pruebas.

La siguiente batería de pruebas fue realizada sobre un equipo con procesador *Intel core2 duo* a 2,2 GHz, y 2 GB de memoria RAM.

	Curvas no Supersingulares			Curvas Supersingulares						
Nº firmas	**160 bits**	**256 bits**	**307 bits**	**128 bits**	**160 bits**	**256 bits**	**384 bits**	**512 bits**	**768 bits**	**1024 bits**
2	0,39890	0,74738	1,00800	0,04459	0,06055	0,11482	0,20433	0,29922	0,5858	0,96008
3	0,51534	0,97887	1,33088	0,05800	0,07642	0,14607	0,27888	0,38235	0,78150	1,29799
4	0,64385	1,22416	1,66541	0,07356	0,09494	0,18202	0,33810	0,47754	0,98135	1,63519
5	0,77129	1,47421	1,99559	0,08433	0,11292	0,21950	0,38474	0,57261	1,17398	1,94974
6	0,89927	1,71999	2,32868	0,09905	0,13200	0,25744	0,44681	0,68585	1,36303	2,30744
7	1,03254	1,96137	2,66144	0,11395	0,15058	0,29448	0,52141	0,76260	1,55099	2,61969
8	1,16332	2,21477	3,00264	0,12703	0,16822	0,33726	0,57768	0,85720	1,73316	2,94449
9	1,29696	2,45331	3,32454	0,14022	0,18672	0,36713	0,63957	0,97010	1,93072	3,25326
10	1,42114	2,69902	3,65905	0,15539	0,20545	0,40293	0,70184	1,05385	2,11347	3,59172
11	1,54459	2,94639	3,99077	0,16808	0,22486	0,44731	0,76985	1,15011	2,31103	3,90204
12	1,67157	3,19075	4,32335	0,18183	0,24198	0,47806	0,83810	1,24213	2,53878	4,21898

Tabla 4-3 Tiempo en segundos de procesado de las firmas

Como se puede apreciar en la Tabla 4-3, el tiempo necesario para realizar la verificación de diez firmas no llega a un segundo y medio para las curvas seleccionadas de 160 bits en el caso de las no supersingulares, por tan sólo 1,05 segundos en el caso de la curva supersingular (con el tamaño de clave de 512 bits para comparar niveles de seguridad equivalentes). Como vemos, se sigue manteniendo una proporción de diferencia de tiempo de procesado entre ambos tipos de curva, similar a la de la batería de pruebas anterior, en torno a un 35%, si bien se han reducido sensiblemente los tiempos de procesado, como se observa en la Fig. 4-10.

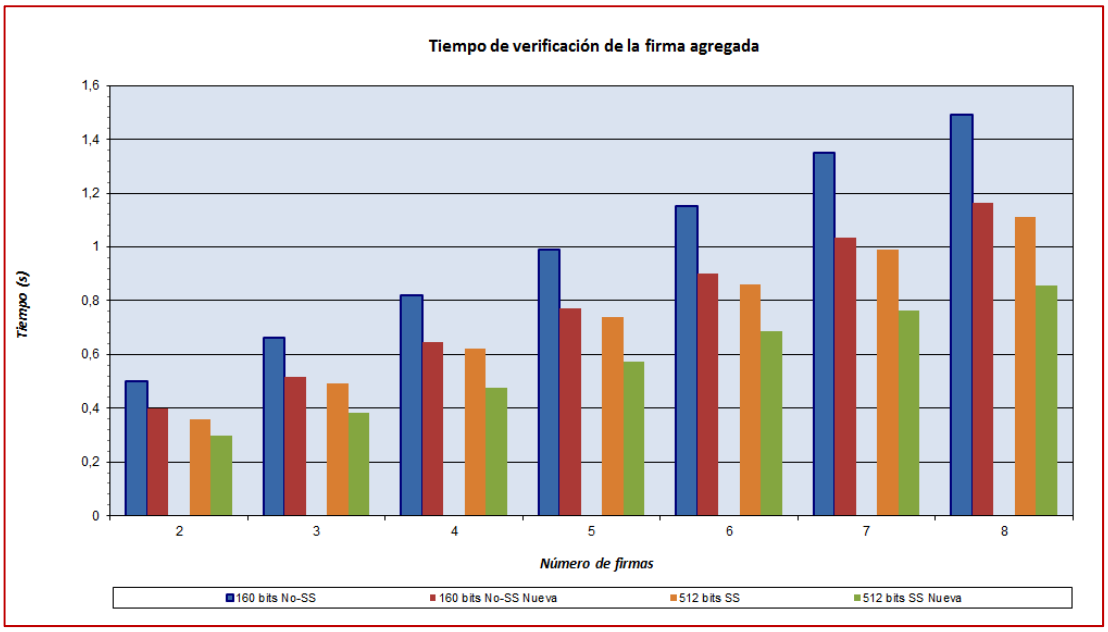

Fig. 4-10. Comparación de tiempo entre la primera y la segunda baterías de pruebas

En la Fig. 4-10, las series correspondientes a la segunda batería de pruebas, se han señalado con la palabra "Nueva". Esta reducción de tiempo de procesado entre la primera y la segunda batería de pruebas, de media un 22%, es achacable al avance tecnológico, principalmente del hardware sobre el que se realizan las pruebas. Para los casos seleccionados, la reducción media del tiempo de procesado ha sido de un 22% en el caso de la firma de 160 bits sobre una curva no-supersingular, y de un 21% en el caso de la firma de 512 bits sobre curva supersingular.

En el prototipo en el que se implementa el sistema, el número máximo de firmas a compactar será tres, por lo tanto, el tiempo medio de verificación será de 0,4 segundos en el caso de las no supersingulares y 0,3 segundos en el caso de las supersingulares.

4.3.1.3. Compatibilidad de los tiempos de procesado con sistema

El tiempo medio que requiere cada uno de los puntos de control varía de manera considerable, no se requiere el mismo tiempo para introducir los datos de cada uno de los animales a su recepción que en verificar el peso de cada una de las piezas de jamón.

Después de analizar los distintos *checkpoints*, se ha comprobado que los tiempos de verificación de la firma, introducción de atributos y generación de la nueva firma agregada son compatibles con la velocidad de la cadena de producción.

Si se exportara el sistema a otra cadena de producción, en la que los tiempos de control fueran menores, como ocurrirá en cadenas automáticas de montaje, se podría variar el tipo de curva y longitud de clave, para ajustar los tiempos y nivel de seguridad a los nuevos requerimientos.

Otra posibilidad, en el caso de que un punto de control requiriese un tiempo menor para la verificación de la firma, sería omitir la verificación de la firma en ese punto concreto delegando la responsabilidad de la verificación al siguiente punto de control.

4.4. Implementación de la aplicación

En este apartado se van a describir los diferentes elementos que constituyen el sistema de firmas agregadas.

4.4.1. Esquema del sistema

El sistema consta de tres partes principales:

- el módulo de administración de usuarios y claves.
- el módulo de verificación y gestión de firmas.
- los clientes que envían datos para verificar las firmas y agregar nuevos mensajes a las etiqueta.

En la figura de la página siguiente, se puede ver una representación esquemática de este sistema.

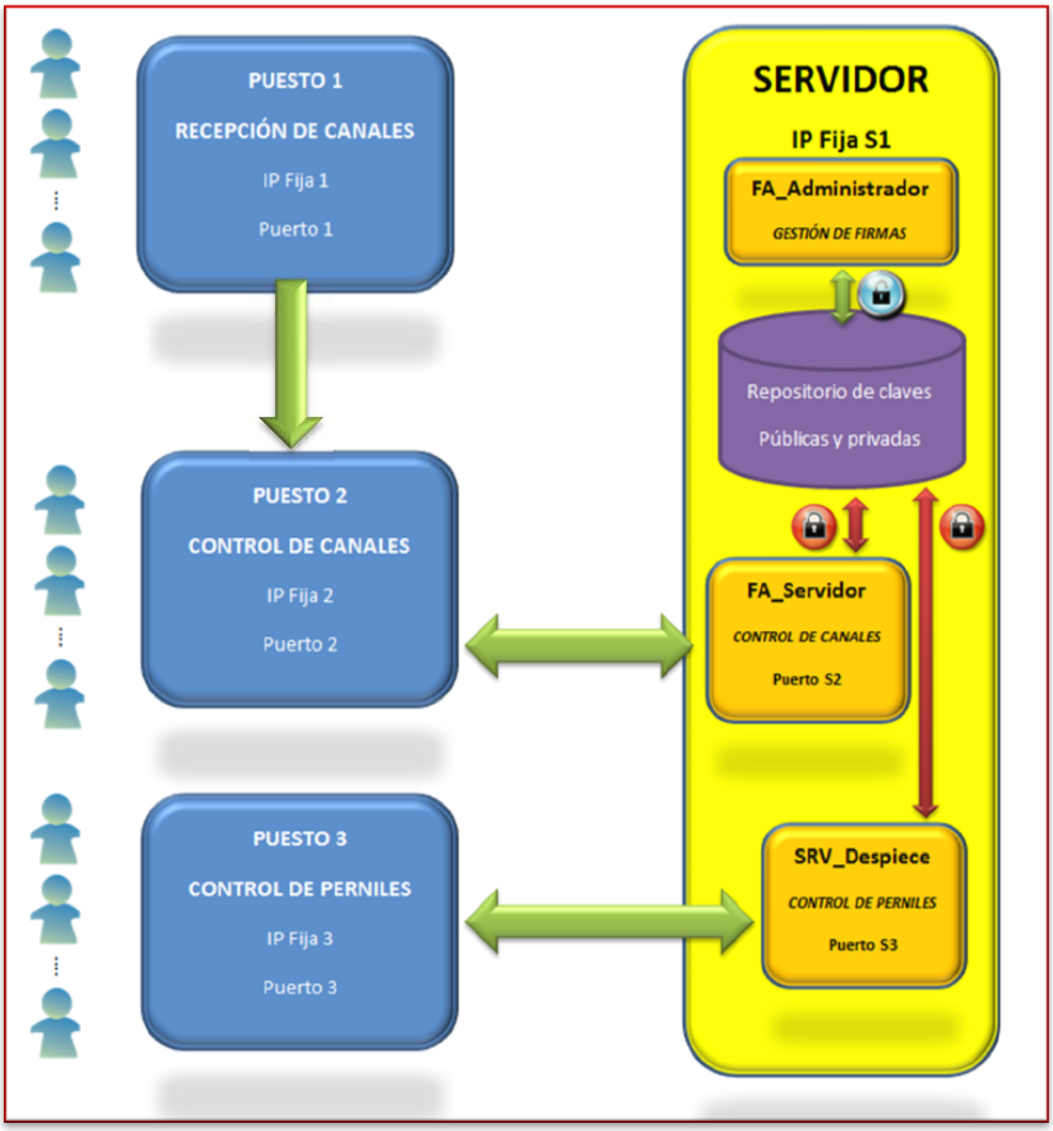

Fig. 4-11. Arquitectura del sistema

En la Fig. 4-11 se representa la arquitectura descrita, representándose con color rojo y un candado cerrado las operaciones de sólo lectura (no permitida la escritura).

La comunicación entre los usuarios de los diferentes puntos del proceso (control de canales y control de perniles) y el servidor de firmas se realiza mediante una arquitectura cliente-servidor, basada en la utilización de sockets sobre una red local TCP/IP.

Cada usuario, que previamente ha debido ser dado de alta en el sistema mediante el módulo Administrador, se debe autenticar frente al sistema mediante un *login* (nombre de usuario) y un *password* (contraseña). Las claves privadas de firma no se le proporcionan al usuario sino que se quedan en el propio servidor de firmas, de manera que las claves privadas nunca viajan por el sistema.

En el servidor de firmas se ejecutan dos aplicaciones (FA_Servidor y SRV_despiece), que son las encargadas de comprobar y generar las firmas requeridas en los puestos control de canales y control de perniles. Cada aplicación está escuchando un puerto distinto, por lo que la aplicación cliente de cada puesto de control se comunicará solamente con la aplicación encargada de ese punto.

Para la gestión de usuarios se ha desarrollado la aplicación FA_Administrador, que se encarga de la gestión de usuarios y claves y que se detallará a continuación. Esta aplicación es la única que tiene permisos para modificar el repositorio de información de usuarios, donde se almacenan los datos de los usuarios y sus claves públicas y privadas. El resto de aplicaciones sólo pueden consultar las tablas para las que tienen autorización, y en ningún caso pueden modificar los datos.

Como optimizaciones implementadas podemos destacar:

- Poner la firma al principio de la tarjeta, debido a que para hacer las firmas y las verificaciones siempre es necesario enviar el mensaje y la firma. Además a la hora de grabar la firma con la impresora RFID, al ser ésta de acceso secuencial y no aleatorio, y estar la firma al principio del espacio de memoria, no es necesario recorrer ningún bit para llegar hasta ella, lo que redunda en un ahorro de los tiempos.

- Codificar los firmantes para ahorrar espacio en las tarjetas RFID (se identifica cada firmante con un número de 1 a 255, es decir con un byte de memoria). Se puede por tanto tener un número máximo de firmantes activos de 255, pero puede haber cualquier número de firmantes (en el siguiente apartado se detallará la gestión de los firmantes). Esta mejora requerirá necesariamente que todos los mensajes que se vayan añadiendo en cada punto de control, contengan un bloque de 4 bytes con la fecha en la que se realiza la firma.

4.4.2. Desarrollo de la aplicación

4.4.2.1. Gestión de usuarios y claves: FA_Administrador

Esta aplicación permite la gestión de usuarios y perfiles que pueden realizar o verificar las firmas agregadas requeridas por el sistema.

Las opciones disponibles para el administrador son:

1. Crear nuevo usuario.
2. Crear nuevo perfil.
3. Agregar perfil a un usuario.
4. Quitar perfil a un usuario.

4.4.2.2. Control de canales: FA_Servidor.

Esta aplicación es la encargada de realizar la primera firma del sistema. En este primer punto, el agente de control tiene en su puesto una consola donde tiene precargada la información de las piezas cuyos atributos debe verificar (estos datos se han introducido en el punto "recepción de canales").

Una vez que el agente de control, que debe estar autenticado, ha realizado las comprobaciones introduce los datos en el sistema. En ese momento la aplicación cliente del *checkpoint* control de canales, le pasa un mensaje con todos los atributos que se han verificado en ese punto, así como los que se habían precargado en el punto anterior. Con todos los atributos y con el identificador del agente de control, la aplicación servidor (FA_Servidor) recupera la clave privada del agente de control, calcula la primera firma y devuelve al cliente un mensaje (en el que se incluyen los atributos, el código del firmante, la fecha y la hora) y la firma del mensaje.

Una vez que se posee la firma, la aplicación cliente graba los atributos, el identificador del agente de control y la fecha y la hora tanto en la etiqueta RFID como en el sistema de información.

4.4.2.3. Control de perniles: SRV_Despiece.

Esta aplicación es la encargada de verificar la firma añadida en el punto anterior (en este punto sólo es una), agregar los nuevos datos y generar una nueva firma.

La aplicación cliente de este *checkpoint* le pasa a la aplicación servidor (SRV_Despiece) el mensaje anterior y su firma correspondiente. El servidor extrae del mensaje el código de identificación del agente de control, la fecha y la hora, lo que le permite recuperar la clave pública del firmante y procede a verificar la firma. Además le pasa los nuevos atributos que se han verificado en ese punto de control.

Si la verificación de la firma es positiva, agrega los nuevos atributos, el identificador del agente de control, la fecha y la hora y calcula la nueva firma con la clave privada del agente de control. La nueva firma agregada sobrescribe a la que había anteriormente en la tarjeta y se envía también al sistema de información.

Si la verificación de la firma es negativa, devuelve una firma con todo ceros, para que quede constancia física fácilmente detectable de que ha habido un problema con la firma.

4.5. Seguridad: aportaciones del sistema frente a amenazas conocidas

A la vista de las amenazas planteadas, ver apartado 2.2.2.2, se van a estudiar las que con mayor probabilidad pueden afectar al prototipo, y qué medidas de protección se han adoptado.

Como se puede apreciar en la Fig. 4-12, en cada punto de control hay un lector/grabador de RFID conectado a un ordenador, donde se ejecuta un módulo de seguridad que verifica la corrección de la firma agregada anterior antes de procesar los nuevos datos, generar la nueva firma y guardarlos tanto en el etiqueta RFID como en el repositorio de información.

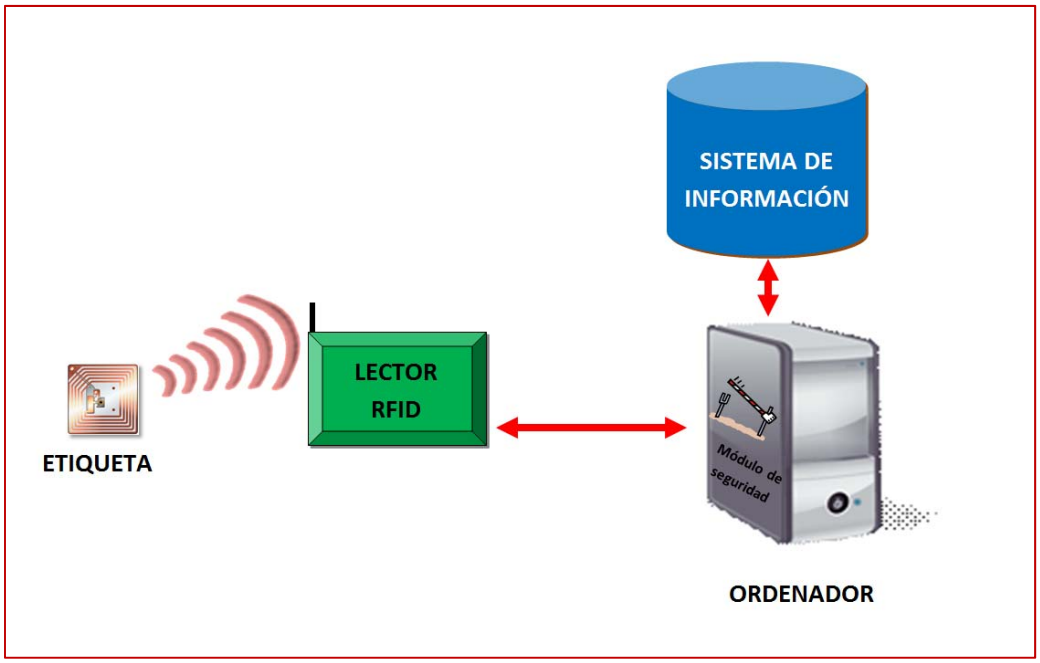

Fig. 4-12 Arquitectura en cada punto de control

4.5.1. La capa física

Dentro de los riesgos asociados a la capa física, cabe señalar que pudiera ocurrir que durante el proceso alguna etiqueta se desprenda o se dañe. En este caso, en el primer punto de control en que se detecte el fallo o ausencia de etiqueta, se comprobará en el sistema de información hasta donde se ha realizado el proceso, se generará una nueva etiqueta con toda la información y se continuará el proceso desde ese punto.

Esto es posible porque en todos los perniles (las piezas sobre las que se desarrolla este proceso) va marcado con tinta, y en un lugar visible, un número identificativo denominado "ROL", y que hace factible la recuperación de los datos asociados a esa pieza aún en el caso de que se haya desprendido la etiqueta.

Otra posible amenaza, es el uso por parte de un atacante del comando KILL [Auto-ID Center2003c][Auto-ID Center2003b] o el comando DESTROY [Auto-ID Center2003a], con el objeto de inutilizar las etiquetas. Creados inicialmente para defender la privacidad del futuro comprador una vez que adquiera el producto, inutilizan permanentemente la tarjeta [JUELS2003]. En el caso que nos ocupa, no es necesario su uso ya que la etiqueta utilizada en esta fase del proceso

no está previsto que llegue al usuario final, y por tanto no se debe implementar medidas especiales para garantizar la privacidad de los consumidores.

Idéntico tratamiento se sigue para el comando LOCK [AYOADE2007], creado para una inhabilitación temporal o permanente de la escritura. Es importante destacar que ya en 2006 algunos autores como Bolan [BOLAN2006] mostraron la posibilidad de que el estado de inhabilitación permanente de una tarjeta fuera reversible. Para más información sobre ataques utilizando estos comandos se recomienda la lectura de [EL-SAID2009].

Respecto a las interferencias activas, parece complicado que un supuesto atacante las pudiera crear, ya que el proceso se realiza siempre en instalaciones privadas, por lo que será suficiente con observar las medidas de protección físicas propuestas en [KARYGIANNIS2007] como son: el control de accesos, cámaras de seguridad, vigilantes y medidas en esta línea. No obstante, se dispone de un plan de contingencia para en el caso de que algún punto de control del sistema de trazabilidad falle, se pueda seguir realizando el proceso productivo y de toma de datos.

La posibilidad de ataques de repetición, como el propuesto en [KFIR2005], es complicada debido a la propia naturaleza de las instalaciones y a las cortas distancias de comunicación entre etiquetas y lectores. Por otro lado, el uso de identidades de calidad (avaladas por una firma electrónica), protege al sistema de una posible alteración maliciosa de los datos, ya que todos van protegidos por la firma. Por todo ello es altamente improbable una alteración de los datos sin que sea detectada por el sistema.

Al hilo de lo anterior, la amenaza más preocupante por su impacto sería la de una clonación de etiquetas; clonarla con la misma apariencia física es complicado (pero no imposible), ya que implica fabricar idéntico modelo de etiqueta con el mismo número de identificación, y por definición es algo que no deberían hacer los fabricantes. Sí que es cierto que existen etiquetas reprogramables, pero si son distintas estéticamente a las legítimas no sería factible su utilización. Además, estas etiquetas clonadas deberían introducirse en el mercado cuando el producto acabe el proceso de producción, ya que de lo contrario serían fácilmente detectables por el sistema. Como impreso de forma visible en la etiqueta RFID figura el número de "ROL", deberían marcarse todas las piezas falsificadas con el mismo número, lo que sería fácilmente detectable a simple vista. Accediendo a los datos de la etiqueta, y suponiendo que la etiqueta fuera una clonación de una etiqueta válida, la identidad se correspondería con una sola pieza, y sería

detectable el fraude. Aun así y si se desea aumentar el nivel de seguridad, se podría recurrir a soluciones hardware basadas en la utilización de funciones físicamente inclonables (PUFs) [BOLOTNYY2007, DEVADAS2008, JENG2009].

En el caso de que se clonaran etiquetas similares pero con distinto número de identificación único serían inmediatamente detectadas ya que la firma agregada incluye el identificador único, y por tanto si la tarjeta no es la misma el identificador cambia y es automáticamente detectado que la firma no es correcta. La clonación de etiquetas es un tema que preocupa de especial manera a los fabricantes, dado que daña la imagen del fabricante y perjudica al usuario, al obtener éster un producto de menor calidad de la esperada [MATOS2007]. Existen muchas propuestas de sistemas o protocolos para detectar la clonación [KHOR2010, MIROWSKI2007, ZANETTI2010] o cómo evitarla [ABAWAJY2009, DUC2006, EL-SAID2009, JENG2009, JUELS2005, LAURIE2007, TUYLS2006].

4.5.2. La capa de red y transporte

Dado que en la etiqueta no hay ningún dato cifrado, no hay ningún problema en que alguien lea el contenido de la tarjeta. En el mismo sentido, si un lector/escritor RFID malicioso escribiera una tarjeta, sería detectado en el siguiente punto de control, dado que no sería capaz de realizar una firma válida.

Este principio se aplica tanto a los ataques que relacionados tanto con la capa de red como con la de transporte.

4.5.3. La capa de aplicación

Como se ha comentado en el punto anterior, no existe ningún problema con las lecturas no autorizadas ya que toda la información va en texto plano, y como también se ha señalado, la modificación de los datos avalados por la firma del agente de control es automáticamente detectada por el módulo de seguridad.

Aunque en la clasificación de riesgos que estamos utilizando se habla exclusivamente de desbordamientos de buffer e inyección maliciosa de código, podríamos hablar en general de malware específicamente diseñado para atacar los sistemas RFID [RIEBACK2008], es decir software diseñado para causar daños en los sistemas. Dentro del malware tenemos tres tipos principales: explotación

de vulnerabilidades conocidas de RFID (RFID *exploits*), gusanos RFID y Virus RFID [RIEBACK2008].

Partiendo de las principales amenazas citadas por [MITROKOTSA2010, MITROKOTSA2009, RIEBACK2008], el mayor peligro de los *exploits* en RFID, es precisamente que muchas veces no son esperados, y su procesamiento puede explotar vulnerabilidades tanto del sistema RFID, como del propio sistema de información o la red entera. El uso de las firmas agregadas en la identidad digital del producto, garantiza que los datos han sido introducidos por entidades autorizadas, por lo que si la firma no es correcta no se pasarán los datos al sistema de información, y el módulo de seguridad descartará los datos y por tanto no ejecutará el comando malicioso.

Otro tipo de ataque dentro de los *exploits* es la inserción de código. Para prevenir esto, y dado que normalmente estos códigos utilizan caracteres distintos a números y letras, una primera medida implementada en las aplicaciones de los puntos de control es que el sistema no procesa ninguna entrada que posea elementos que no sean números y letras. Adicionalmente, como en el caso anterior, el módulo de seguridad filtra los datos que llegan al sistema de información. Tampoco se permite la ejecución de lenguajes script en el sistema *back-end*.

No menos peligroso es un desbordamiento de buffer (*buffer overflow*) que se produce cuando en un área de memoria se escriben más datos de los que puede contener, y estos sobrescriben zonas de memoria anexa. En [RIEBACK2008] se presenta un ejemplo de desbordamiento en un sistema RFID. En este caso, el filtrado previo del módulo de seguridad a través de la confirmación de la validez de la firma, hace que los datos maliciosos no lleguen al sistema de información.

Los gusanos RFID se basan en la explotación de fallos de los sistemas para introducir código malicioso en el lector que sobrescribirá las tarjetas con un código que cuando sean leídas provocará la infección de un nuevo lector que a su vez infectará nuevas tarjetas. Nuevamente la comprobación previa de las firmas impedirá la propagación de la infección mediante las tarjetas, pero si se detectara alguna actividad de este tipo se auditará la seguridad del sistema para saber cómo ha sido infectado el lector (probablemente vía red). En este caso, es importante volver a señalar la importancia de una política de seguridad adecuada que afecte a todos los sistemas implicados en el proceso (para ampliar la información se recomienda la consulta de ISO/IEC 17799:2005 e ISO 27002:2005).

Incluso tratándose de virus sofisticados, con las normas generales básicas habituales que se han aplicado, como limitar los permisos de la base de datos y de los usuarios, aislar el servidor middleware del resto de la red y revisar el código del middleware para evitar agujeros de seguridad [CLARKE2009a, CLARKE2009b], se obtiene un nivel de seguridad elevado.

4.5.4. La capa estratégica.

De los riesgos comentados (espionaje industrial, técnicas de ingeniería social, amenazas a la privacidad, selección de objetivos) sólo afecta al sistema, en alguna medida, la posibilidad de que mediante técnicas de ingeniería social, se consiga que algún agente de control realice alguna acción que pudiera comprometer el funcionamiento del sistema. Las contramedidas implementadas son: la formación adecuada del personal y la definición de una política general de seguridad. Además aquí no existe la posibilidad de acceso directo a las claves privadas de firma por parte de los usuarios, es decir, cuando un usuario legítimo inicia la sesión se debe autenticar, y será el servidor de firmas el que realice los cálculos, no teniendo acceso directo el agente de control a su clave privada de firma en ningún momento.

4.5.5. Ataques multicapa.

Aunque la estructura de estos ataques es similar a sus homónimos en capas individuales, en este caso pueden implicar a varias capas. Los ataques que se estima pueden afectar al sistema presentado son: denegación de servicio, la lectura / escritura de información en el espacio libre de la tarjeta sin autorización y ataques de repetición. El resto, dado que en nuestro sistema no es necesaria privacidad no afectan.

Los ataques de denegación de servicio (DoS) podrían afectar a la cadena de producción, no obstante para su ejecución haría falta acceso físico a los recintos, por lo que las medidas físicas propuestas en el subapartado 4.5.1 deberían ser suficientes. No hay que olvidar que dada la existencia de redes de comunicaciones en el sistema, estas sí son vulnerables a ataques externos de DoS, por lo que se han tomado las medidas de seguridad habituales para evitar este tipo de ataques.

La protección frente al resto de ataques citados ya ha sido comentada en los puntos anteriores.

4.6. Análisis económico

Para finalizar este capítulo, se ha considerado incluir un análisis de los beneficios económicos que puede producir la aplicación del sistema propuesto en un entorno productivo que genere cantidades elevadas de productos (del orden de algunos cientos de miles al año).

Según se señala en [SARAC2010], un ROI (*Return-on-investment*) positivo, depende de los costes de la tecnología (el precio de las etiquetas, coste del servicio de mantenimiento, etc…). En el árbol de costes planteado en [BANKS2007], los costes se dividen en: costes de proceso de reingeniería (costes de personal), costes de instalación del servicio, costes de integración del sistema, costes de *software* y costes de *hardware*. Dentro de estos últimos, se computan los costes de: lectores RFID, etiquetas, antenas, cableado y conectores, ordenadores y dispositivos de red.

El uso del sistema propuesto, ofrece una importante disminución en la inversión en etiquetas RFID, debido tanto a los menores requerimientos de espacio de memoria como a no necesitar etiquetas securizadas, lo que posibilita adquirir etiquetas muy económicas. En el estudio de riesgos en la implantación de un sistema RFID realizado por [XIAO2010], se apunta directamente al coste de las etiquetas como el riesgo más importante de implantación del sistema (junto con el coste global de la solución y la privacidad personal), coincidiendo en este aspecto otros trabajos como ([ANGELES2005, BOTTANI2008, JONES 2004, WU2005]. Además, este ahorro se produce durante toda la vida útil del sistema, ya que la adquisición de etiquetas es constante mientras se esté utilizando.

En la Fig. 4-13, se muestra una estimación de la inversión en etiquetas RFID dependiendo de: el número de firmantes, el tipo de protocolo utilizado para la firma, el número de piezas y el coste por unidad de cada etiqueta. Como se puede apreciar en la gráfica, en el caso de la utilización del sistema propuesto, el tamaño de la firma se mantiene constante independientemente del número de firmantes. Esta característica, reduce el coste del sistema de manera importante frente a los esquemas basados en firmas individuales (una firma por cada mensaje), y que requieren una cantidad mucho mayor de memoria.

También hay ocasiones en que las características específicas de la propia tarjeta (resistencia a determinadas condiciones de humedad, temperatura, corrosión, etc…), hace que no existan en el mercado etiquetas con la cantidad de memoria requerida, y que por ejemplo el tamaño máximo disponible sea de 2K, lo que condicionará fuertemente el planteamiento del sistema. Es importante

señalar, que habitualmente no todo el espacio de memoria que ofrece la etiqueta puede ser utilizado libremente, sino que hay una serie de bloques reservados. Por ejemplo, en la etiqueta que se utilizó en el prototipo, de los 1024 bits que tiene de memoria, sólo pueden ser utilizados libremente 640 bits (20 bloques). En un caso como este, con el uso del sistema propuesto, podría paliarse el problema, ya que el requerimiento de espacio de memoria para la firma es mucho menor. Esta circunstancia se presentó durante el desarrollo del prototipo. Con la tarjeta seleccionada ni siquiera cabría una firma utilizando RSA, porque el tamaño de firma para el nivel de seguridad requerido es de 1024 bits, y las etiquetas que soportan las características del proceso productivo tienen una memoria utilizable de 640 y deben guardarse el resto de atributos de la identidad, además de la firma.

Para realizar un pequeño análisis, se va a tomar el número anual de piezas etiquetadas por el Consejo Regulador de la Denominación de Origen Jamón de Teruel, por ejemplo los que corresponden al año 2009, que ascendieron a 675.276 (la mayor producción nacional con marchamo de calidad). Además, se puede suponer que se van a añadir tres firmas. También hay que considerar, que en las etiquetas de 1K sólo quedan libres 8 bloques, es decir 256 bits. Para el mismo nivel de seguridad requerido, las alternativas analizadas han sido: firmas individuales para cada mensaje RSA de 1024 bits, firmas individuales para cada mensaje ECDSA de 160 bits y el uso de firmas agregadas de 163 bits propuesto. Obteniendo los siguientes resultados:

Esquema de firma	Espacio ocupado (bits)	Tipo de tarjeta Necesaria	Coste por tarjeta (€)	Coste anual (€)
RSA 1024	1024 x 3	4 K	0.91	614.501,16 €
ECDSA 160	160 x 3	2 K	0.68	459.187,68 €
Firma Agr.	163	1 K	0.29	195.830,04 €

Tabla 4-4. Coste anual para tres firmantes en función del tipo de etiqueta

Como se puede ver en la Tabla 4-4, el ahorro anual que se produce para las condiciones citadas es de un 57 % (263.357,64 €) respecto a ECDSA 160 y de un 68 % (418.671,12 €) respecto a RSA 1024.

Extendiendo este mismo análisis, con el mismo número de piezas anuales, a una cadena de producción con hasta 7 firmantes, se obtienen los siguientes resultados, mostrados en las Fig. 4-13 y Fig. 4-14 :

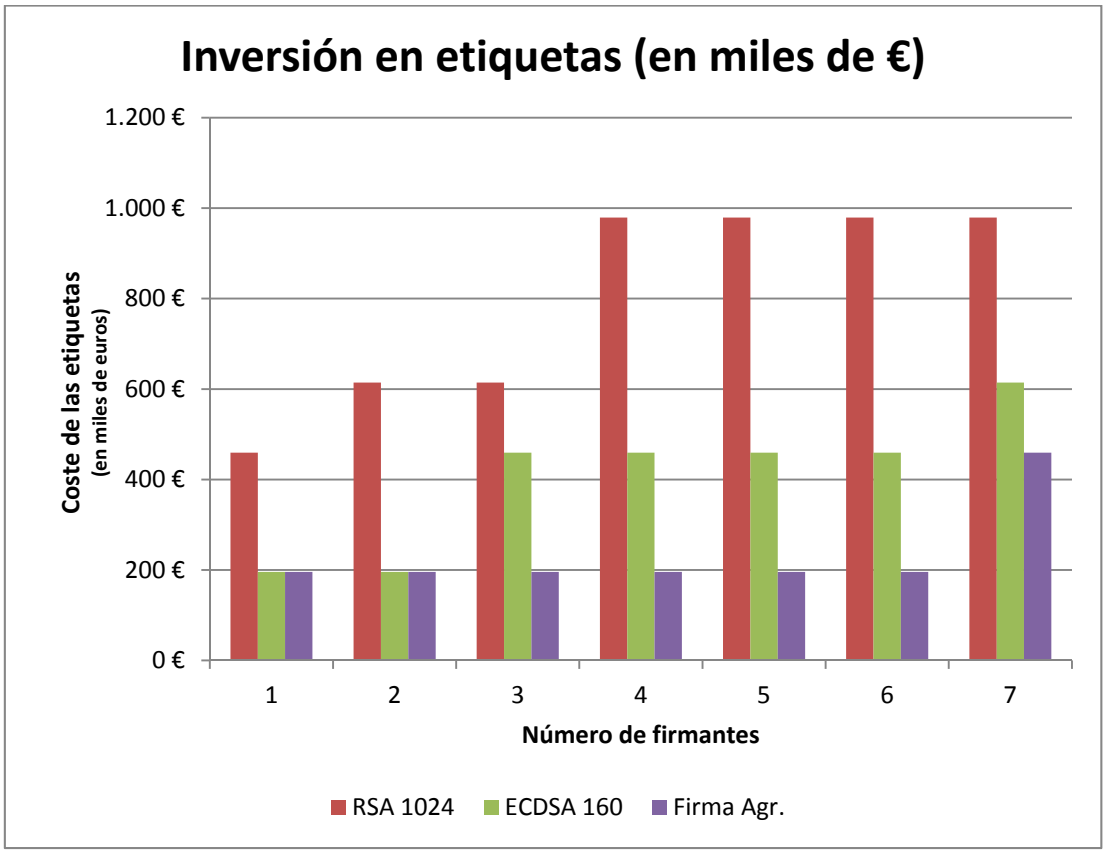

Fig. 4-13. Inversión en etiquetas en miles de €

Como se observa en la Fig. 4-13, la inversión necesaria en etiquetas es mayor en RSA para cualquier número de firmantes. Respecto a ECDSA, se observa que hasta dos firmantes el coste es el mismo que en el caso de las firmas agregadas, entre tres y seis firmantes el coste vuelve a ser claramente superior (más del doble) y finalmente en el caso de siete firmantes aunque sigue siendo más ventajoso el uso de firmas agregadas, la diferencia se reduce considerablemente respecto al caso anterior.

En la Fig. 4-14, se presenta el ahorro en miles de euros al año que supone el uso de la firma agregada frente a RSA o ECDSA.

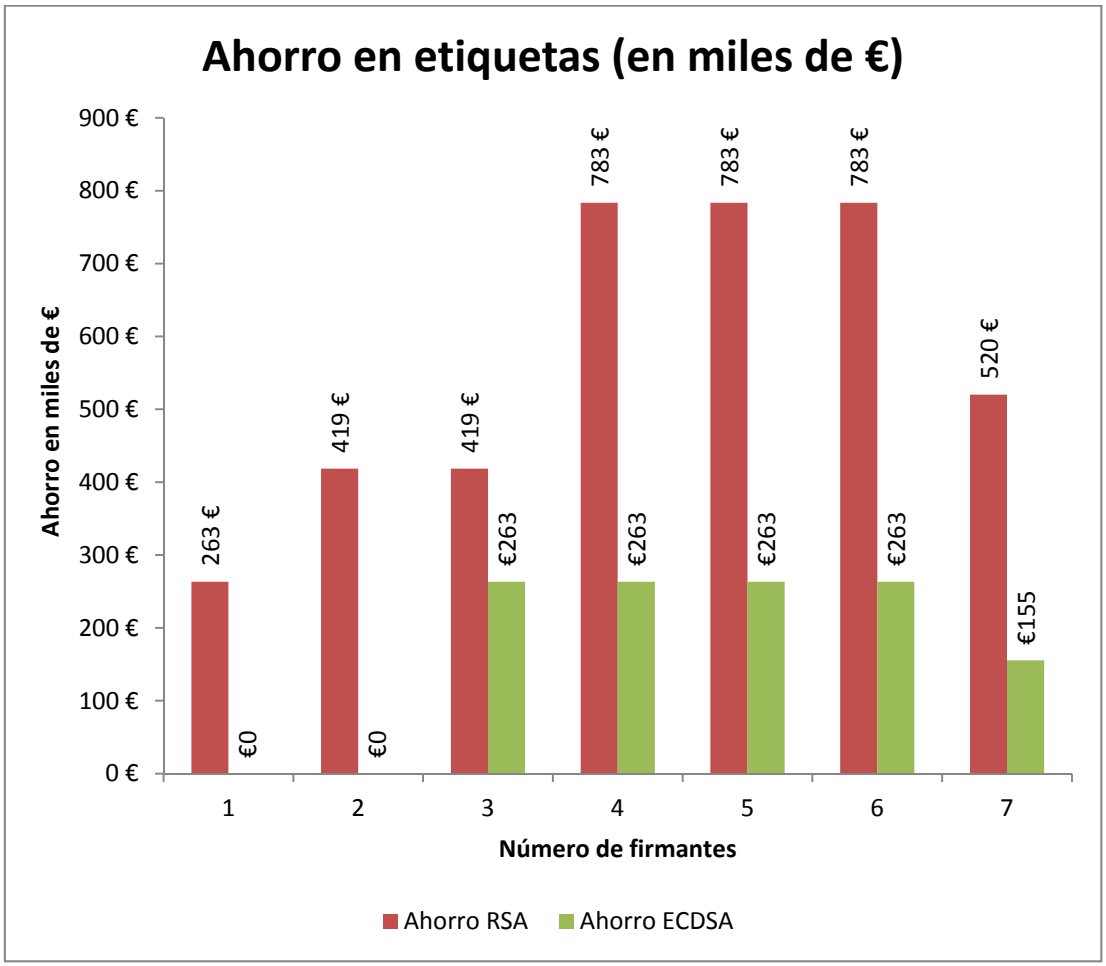

Fig. 4-14. Ahorro en etiquetas en miles de € anuales.

5. Conclusiones y Líneas Futuras de Investigación

5.1. Conclusiones

Como conclusiones cabe destacar en primer lugar que se ha cumplido el objetivo principal de la tesis: el estudio y diseño de un sistema de identidad digital basada en atributos avalados por entidades confiables; siendo la autenticidad de la identidad fácilmente verificable a partir de las claves públicas de los emisores de opinión.

Se ha realizado una prueba de concepto, dotando de garantía a un sistema de trazabilidad alimentaria basado en RFID. En este sistema cada pieza es identificada a través de una serie de medidas objetivas, introducidas como atributos en el sistema por un agente de control autorizado, y que se graban en una etiqueta RFID que acompaña al producto.

Se ha desarrollado una alternativa a los sistemas de criptografía ligera embebidos en las etiquetas RFID, que puede ser utilizada con etiquetas de ultra-bajo coste. Para trabajar con este tipo de etiquetas se ha recurrido al reducido tamaño de firma que proporciona el uso de criptografía de curvas elípticas y firmas agregadas, lo que ha permitido reducir considerablemente la cantidad de bits que se deben almacenar en la etiqueta RFID, respecto a otras soluciones criptográficas, para un mismo nivel de seguridad. Económicamente, dado que el sistema utiliza etiquetas RFID no securizadas y tamaños de firma relativamente pequeños, el ahorro en etiquetas es importante.

Otra característica interesante es que una tercera parte no relacionada con el sistema, que posea un lector RFID y las claves públicas de los firmantes puede comprobar y verificar de forma sumamente sencilla la autenticidad de los datos. Esto, por supuesto, también incluye a todas las personas involucradas en la cadena de producción y distribución de los productos, lo que facilita la confianza entre diferentes empresas involucradas en un proceso de fabricación.

El sistema es totalmente escalable, lo que permite su uso en un proceso de producción largo, en el que incluso intervengan diversas compañías, siempre que haya un ente, que puede ser creado ad-hoc para un proceso concreto, que se encargue de la gestión de las claves.

También se ha desarrollado, un sistema de gestión automática de la confianza en los agentes de control, basado en la variación de su reputación a lo largo del tiempo, como consecuencia de la correcta o incorrecta realización de sus tareas.

Respecto a las limitaciones del sistema, son básicamente dos:

- La primera es que por el tema de costes se ha propuesto el uso de etiquetas estándar sin securizar, por lo tanto no se ha implementado ningún mecanismo adicional para evitar su clonación.
- La segunda limitación del prototipo es que aunque es escalable, se ha probado en un proceso real pero corto. De haber podido probarse en un proceso más largo se hubieran obtenido datos de mayor interés sobre el rendimiento del sistema.

En definitiva, se ha conseguido un sistema de confianza exportable basado en una identidad de calidad, ya que se adapta a cualquier entorno de producción, y permite las relaciones de confianza entre empresas con un mínimo intercambio de datos, habiéndose comprobado su viabilidad en un prototipo.

5.2. Líneas futuras de investigación

Como líneas futuras de investigación, se propone probar el sistema en otro tipo de cadenas de producción, para ver su rendimiento e intentar mejorarlo, ya que se cree que el sistema es aplicable a cualquier tipo de proceso de producción en el que haya puntos de control intermedio durante su fabricación. Además, y aunque el coste de la implantación del sistema no es muy elevado, se podría trabajar en el estudio de medidas para reducir los costes de implantación y explotación del sistema, para facilitar su uso en cadenas de producción de productos de menor valor añadido.

Para facilitar la verificación de las piezas por parte del cliente final (el consumidor), y dado que en la actualidad los consumidores domésticos no suelen disponer de lectores RFID, en el último paso del proceso se podría incluir la identidad en un código QR, de manera que con ayuda de un portal web, se pudiera comprobar la autenticidad de la identidad. Esto supondría además un importante *feedback*, especialmente útil en la relación de confianza agente de control - empresa. En esta misma línea y con el mismo propósito de facilitar al cliente el acceso a la información, también podría incluirse en la última fase del proceso la información en una etiqueta NFC.

La constante investigación en criptografía ligera y ultra-ligera lleva a pensar que quizás a corto o medio plazo se pudiera implementar una versión ligera de

este sistema en las propias etiquetas RFID, sin necesidad de realizar los cálculos en un sistema externo y asumiendo que éstas tendrían un coste que si bien no sería posible su utilización en productos de coste moderado, sí podrían utilizarse en productos de lujo como garantía de su proceso de producción especialmente cuidado y distintivo de su calidad.

Anexo I. Glosario trazabilidad.

Una parte muy importante de la trazabilidad está relacionada con la normalización y el intercambio de información entre diferentes partes, por lo que a continuación, se presenta un glosario con términos relacionados con la trazabilidad y que serán utilizados a lo largo del trabajo. Las siguientes definiciones están extraídas de la monografía [AESAN2009]:

- ***Auditoría:*** *Un examen sistemático e independiente para determinar si las actividades y sus resultados se corresponden con los planes previstos, y si éstos se aplican eficazmente y son adecuados para alcanzar los objetivos.*

- ***Cliente****: La siguiente persona u operador económico en la cadena alimentaria a quien se vende o facilita el alimento.*

- ***Consumidor final****: el consumidor último de un producto alimenticio que no empleará dicho alimento como parte de ninguna operación o actividad mercantil en el sector de la alimentación.*

- ***Control****: La realización de una serie programada de observaciones o mediciones a fin de obtener una visión general del grado de cumplimiento de la legislación sobre piensos y alimentos, así como de la normativa en materia de salud animal y el bienestar de los animales.*

- ***Control oficial****: Toda forma de control que efectúe la autoridad competente para verificar el cumplimiento de la legislación sobre piensos y alimentos, así como las normas relativas a la salud animal y el bienestar de los animales.*

- ***Empresa alimentaria****: toda empresa pública o privada que, con o sin ánimo de lucro, lleve a cabo cualquier actividad relacionada con cualquiera de las etapas de la producción, la transformación y la distribución de alimentos.*

- ***Empresa de piensos****: Toda empresa pública o privada que, con o sin ánimo de lucro, lleve a cabo cualquier actividad de producción, fabricación,*

transformación, almacenamiento, transporte o distribución de piensos; se incluye todo productor que produzca, transforme o almacene piensos para alimentar animales de su propia explotación.

- ***Incumplimiento**: El hecho de no cumplir la legislación en materia de productos (piensos y alimentos).*

- ***Inspección**: El examen de todos los aspectos relativos a los piensos, los alimentos, la salud animal y el bienestar de los animales, a fin de verificar que dichos aspectos cumplen los requisitos legales establecidos en la legislación sobre piensos y alimentos, así como en la normativa en materia de salud animal y bienestar de los animales.*

- ***Lote**: Conjunto de unidades de venta de un producto alimenticio producido, fabricado o envasado en circunstancias prácticamente idénticas.*

- ***Operador de empresa alimentaria**: Las personas físicas o jurídicas responsables de asegurar el cumplimiento de los requisitos de la legislación alimentaria en la empresa alimentaria bajo su control.*

- ***Operador de empresa de piensos**: Las personas físicas o jurídicas responsables de asegurar el cumplimiento de los requisitos de la legislación alimentaria en la empresa de piensos bajo su control.*

- ***Operador económico**: Operador de empresa alimentaria y/o operador de empresa de piensos.*

- ***Pienso**: Cualquier sustancia o producto, incluidos los aditivos, destinado a la alimentación por vía oral de los animales, tanto si ha sido transformado entera o parcialmente como si no.*

- ***Proveedor**: La persona u operador económico inmediatamente anterior en la cadena alimentaria, quien vende o facilita el alimento.*

- ***Rastreabilidad/rastreo**: Denominaciones alternativas de trazabilidad.*
- ***Trazabilidad**: También llamada rastreabilidad o rastreo. Posibilidad de encontrar y seguir el rastro, a través de todas las etapas de producción,*

transformación y distribución, de un alimento, un pienso, un animal destinado a la producción de alimentos o una sustancia destinados a ser incorporados en alimentos o piensos o con probabilidad de serlo. Capacidad para seguir el movimiento de un alimento a través de etapa(s) especificada(s) de la producción.

- ***Trazabilidad hacia atrás**: También llamada "trazabilidad de proveedores": Posibilidad de conocer qué productos entran en la empresa y quiénes son sus proveedores.*

- ***Trazabilidad interna**: También llamada "trazabilidad de proceso". Trazabilidad de los productos dentro de la empresa (independientemente de si se producen o no nuevos productos).*

- ***Trazabilidad hacia delante**: También llamada "trazabilidad de clientes": Posibilidad de conocer qué productos salen de la empresa y a quién se han vendido o facilitado.*

- ***Validación**: La obtención de pruebas que demuestren que la medida o medidas de control de higiene de los alimentos o piensos seleccionadas para controlar un peligro en un alimento o un pienso son capaces de controlar, de manera constante, el peligro al nivel especificado.*

- ***Verificación**: La confirmación, mediante examen y estudio de pruebas objetivas, de si se han cumplido los requisitos especificados.*

Anexo II. RFID: normativa y estándares.

A continuación, se va a presentar un pequeño resumen no exhaustivo de normativa relativa a RFID. Aunque es una tecnología relativamente nueva, realmente no lo es tanto, su uso se ha ido popularizando durante los últimos años, lo que ha llevado a diversos organismos a desarrollar diversos estándares y documentos de normalización para distintas aplicaciones. Normalmente describen las capas físicas y de enlace de datos, detallando aspectos como los interfaces de comunicación inalámbrica, protocolos anticolisión, protocolos y seguridad.

Entre los estándares más importantes, podemos contar con los siguientes:

- **Identificación animal:**
  - ISO 11784: estructura del código.
  - ISO 11785: Conceptos Técnicos.
  - ISO 14223: Especifica el interfaz aéreo entre el transceptor y el transpondedor con plena compatibilidad con los dos estándares anteriores.

- **Tarjetas inteligentes inalámbricas** (*Contactless integrated circuit(s) cards):* el estándar ISO/IEC 7810:2003 es uno de una serie de estándares que describen las características de las tarjetas de identificación. Su propósito es proporcionar criterios según los cuales las tarjetas se puedan fabricar y especificar los requisitos para que estas tarjetas puedan ser utilizadas en diferentes países. Tiene en cuenta tanto aspectos humanos como técnicos y establece unos requerimientos mínimos. Se han publicado dos correcciones posteriores en 2009 y en 2012.
  - ISO/IEC 10536: para tarjetas que operan a distancias muy cortas del lector (menores de 1 cm.).
  - ISO/IEC 14443: para tarjetas que operan a distancias de unos 10 cm. del lector. Poseen un microprocesador. El estándar tiene diversas partes. La última revisión es del año 2012.
  - ISO/IEC 15693: para tarjetas que operan hasta 1 m.

- **Gestión de objetos:** la norma más importante sea probablemente la **ISO/IEC 18000** presenta unas definiciones y define el interfaz de comunicación inalámbrica, los mecanismos de detección de colisiones, y los protocolos para comunicación en diferentes bandas de trabajo. Tiene 7 partes (aunque la cinco ha sido suprimida).

- **Estándares relacionados con RFID:**
  - ISO/IEC 15961: Protocolo de datos: interfaz de la aplicación.
  - ISO/IEC 15962: Protocolo de datos: normas de codificación de datos y funciones lógicas de memoria JTC 1/SC 31 .
  - ISO/IEC TR 18046: Información tecnológica. Pruebas de rendimiento.
  - ISO/IEC TR 18047: Información tecnológica. Pruebas de conformidad.
  - ISO 18185: RFID para sellado electrónico de contenedores de carga (ISO TC 104 – Contenedores de carga).
  - ISO/IEC 19762: Información tecnológica. Técnicas de identificación y captura de datos automática (AIDC). Armonización de vocabulario. La parte 3 se refiere a RFID.
  - ISO 23389: Contenedores de Carga. (ISO TC 104)
  - ISO/IEC 24730: Información Tecnológica. El propósito del estándar es permitir la compatibilidad y potenciar la interoperabilidad de sistemas de localización en tiempo real RTLS. En la parte 1 se define una interfaz de programación de aplicación, y en la 2 el interfaz de comunicación inalámbrico a 2.4 GHz.
  - ISO/IEC 15434: Información Tecnológica. Sintaxis para transferencia a medios de captura automática de datos (ADC) de alta capacidad.
  - ISO/IEC 15459: Información Tecnológica. Identificadores únicos.
    - Parte 1: Identificación única de unidades de transporte.
    - Parte 2: Procedimientos de registro.
    - Parte 3: Reglas comunes para identificación única.
    - Parte 4: Identificación única por objetos para gestión de cadenas de suministro.

- Parte 5: Identificación única de objetos de transporte retornables (RTIs).
- Parte 6: identificación única para agrupaciones de productos en gestión de ciclo de vida de materiales.

- ISO/IEC 15961: Interfaz entre la aplicación y el protocolo de datos:
  - Parte 1: Interfaz de aplicación.
  - Parte 2: Registro de constructores de datos RFID.
  - Parte 3: constructores de datos RFID.
- ISO/IEC 15962: Protocolo: Reglas de codificación de datos y funciones lógicas de memoria.
- ISO/IEC 15963: Identificación única de etiqueta de Radio Frecuencia.
- ISO/IEC 18001: Perfiles de requerimientos de aplicación (ARP)
- ISO/IEC 18047: proporciona métodos de prueba para verificar la compatibilidad con varias partes del estándar ISO/IEC 18000. Tiene varias partes (2-7) con los parámetros para diversas frecuencias
- ISO/IEC 18046: Test para rendimiento de métodos de etiquetas y lectores RFID.
- ISO/IEC 19762: Información tecnológica AIDC. Armonización de vocabulario.
- ISO/IEC 24710: ha sido diseñado para ayudar a los usuarios a implementar los estándares de comunicación inalámbrica ISO/IEC 18000, con un énfasis particular en las tarjetas más sencillas.
- ISO/IEC 24729: Orientaciones básicas de implementación.
  - Parte 1: etiquetas RFID.
  - Parte 2: reciclabilidad de etiquetas RF.
  - Parte 3: instalación de lector y antena RFID.
- ISO/IEC 24730: Sistemas de localización en tiempo real.
  - Parte 1: Interfaz de programación de aplicación (API).

        - Parte 2: 2.4 GHz.
        - Parte 3: 433 MHz.
        - Parte 4: Sistemas de Localización Global (GLS).
    - ISO/IEC 24752: Protocolo de Gestión de Sistema.
    - ISO/IEC 24753: Comandos de interfaz inalámbrico para bacteria y funcionalidades de sensores.
    - ISO/IEC 24769: Métodos de test para conformidad de dispositivos con RTLS.
    - ISO/IEC 24770: Métodos de test para medir el rendimiento de dispositivos con RTLS.

- **Comunicación de campo cercano (NFC)**: se incluye dentro de este listado porque constituye una forma de identificación por radiofrecuencia. Fue aprobado como un estándar ISO/IEC en Diciembre de 2003 y posteriormente como estándar ECMA. NFC es una plataforma tecnológica abierta descrita en los estándares ECMA-340 e ISO/IEC 18092. Especifican los esquemas de modulación, codificación, velocidades de transferencia y formato de tramas para el interfaz de radiofrecuencia de los dispositivos. También describe esquemas de inicialización y condiciones requeridas para el control de colisiones durante la inicialización tanto del modo pasivo como del activo. Además, define el protocolo de transporte (incluyendo el protocolo de activación y los métodos de intercambio de datos. El interfaz de comunicación inalámbrica está estandarizado en:

    - ISO/IEC 18092 / ECMA-340: Interfaz y protocolo 1 de comunicación de campo cercano, *Near Field Communication Interface and Protocol-1* (NFCIP-1).
    - ISO/IEC 21481 / ECMA-352: Interfaz y protocolo 2 de comunicación de campo cercano, *Near Field Communication Interface and Protocol-2* (NFCIP-2).
    - ISO/IEC 14443: incorporado a NFC tanto el tipo A como el B, así como FeliCa.

- **Código Electrónico de producto (EPC):** fue diseñado como un identificador universal que asignaba una identidad única a cada objeto físico. Su estructura está definida en el estándar EPCglobal Tag Data (la última versión es la 1.6 y es de Septiembre de 2011)**.** Aunque es muy habitual basar el sistema de captura automática de datos en tecnología RFID, el sistema EPC soporta otras tecnologías. Los estándares de EPCGlobal son los siguientes:

    - Descripción de la arquitectura: *Architecture Framework* (v.1.4).
    - Identificación: *Tag Data Standard* v. 1.6 (2011) y *EPC Tag Data Translation (TDT) Standard* v. 1.6.
    - Identificación – Captura: *Class 1 Generation 2 UHF Air Interface Protocol Standard "Gen 2"* (UHF Class 1 Gen 2 Standard v. 1.2.0) y *EPC™ adio-Frequency Identity Protocols EPC Class-1 HF RFID Air Interface Protocol* (EPC HF RFID Air Interface Standard v. 2.0.3).
    - Captura: *Low Level Reader Protocol (LLRP) Standard* (v. 1.1), *Discovery, Configuration & Initialisation Standard for Reader Operations* (DCI Standard v. 1.0), *Reader Management (RM) Standard* (RM Standard v. 1.0.1), *Application Level Events (ALE) Standard* (ALE 1.1.1 Standard).
    - Captura – Intercambio: *EPCIS - EPC Information Services Standard* (EPCIS Standard v. 1.0.1), *Core Business Vocabulary (CBV)* (CBV Standard v. 1.0).
    - Intercambio: *Object Naming Service (ONS) Standard* (ONS Standard v. 1.0.1), *Discovery Services Standard* (todavía en desarrollo), *Certificate Profile Standard* (v. 2.0), *Pedigree Standard* (v. 1.0).

Anexo III. Criptografía ligera en RFID.

Aunque finalmente no han sido utilizadas estas técnicas en el desarrollo de esta tesis, sí que fueron objeto de estudio en la fase inicial y uno de los objetivos de la propuesta de tesis. Se ha decido incluir este apartado como anexo, porque a pesar de que finalmente no ha sido utilizado, el autor considera que hay un interesante repaso a diferentes protocolos que se agrupan en la referida categoría.

La criptología ligera es un campo dentro de la criptología, en el que convergen la ingeniería electrónica, la informática y las matemáticas con el objeto de poder desarrollar primitivas y protocolos, como cifradores de bloques o de flujo, funciones resumen (*hash*), métodos de autenticación e identificación, etc… que sean implementables en dispositivos con escasísimos recursos computacionales y energéticos (como el caso de las etiquetas pasivas de RFID de bajo coste). También se ocupa del criptoanálisis de las primitivas y los protocolos propuestos con el objeto de comprobar su robustez frente a ataques. En [CHAI2012, DAVID2011, PERIS-LOPEZ2008] se puede ampliar la información sobre estas primitivas y protocolos.

A diferencia de la criptografía clásica donde una primera clasificación se hace entre los sistemas de clave simétrica y asimétrica, en la clasificación propuesta en [DAVID2011] se señala que en criptografía ligera actualmente es muy difícil el uso de primitivas asimétricas de clave pública, debido a que los cifradores de clave pública basados en los problemas de la factorización del logaritmo discreto no son adecuados para su implementación debido a su elevado coste [EISENBARTH2007] . Según la bibliografía el único cifrador de clave pública adecuado para las etiquetas RFID es NTRU [EISENBARTH2007], como lo demuestra alguna de las implementaciones [ATICI2008]. Así pues, y dejando de lado las primitivas de criptografía ligera basadas en cifradores de clave asimétrica, David [DAVID2011] propone la siguiente clasificación:

- **Primitivas Físicas**: funciones físicas de un sentido y primitivas de capa física.
- **Primitivas computacionales** (de clave simétrica): cifradores de clave simétrica (de flujo y de bloque) y funciones *hash* con clave (*Keyed Hash Functions).*

- **Protocolos ultraligeros**: Libreta (o relleno) de un solo uso (*one-time pad),* Re-cifrado.

Para finalizar este apartado, se van a describir brevemente algunos sistemas y algoritmos criptográficos que nos deberían permitir verificar la autoría de la introducción de datos en el sistema. En principio, y dado que el volumen de etiquetas a manejar va a ser muy alto y el coste del producto a priori no va a ser extraordinariamente elevado, centraremos la revisión en técnicas de criptografía ligera o ultra-ligera.

Como finalmente, tras la revisión bibliográfica se comprobó que las soluciones existentes no eran viables con los parámetros de coste del tipo de procesos que pretendía abarcar el sistema objeto de esta tesis, se presenta sólo un breve repaso bibliográfico de diferentes servicios de seguridad en criptografía ligera.

Básicamente, la autenticación e identificación debe hacer frente de manera general a los siguientes requisitos fundamentales [CHAI2012]:

- Autenticación (seguridad): después de la ejecución del protocolo, el lector puede identificar una etiqueta legítima con certeza.

- Anonimato (privacidad): el protocolo entre el lector y la etiqueta no debe permitir la obtención del número de identificación de la etiqueta (o de un pseudo-ID).

- Impedir la trazabilidad, *untraceability* (privacidad): un adversario no debe saber que una transacción ha involucrado a una determinada tarjeta después de un determinado tiempo. Este requisito satisface el deseo de los usuarios que prefieren que una vez han realizado la adquisición del producto, no desean que este siga siendo objeto de registro por parte de sistemas de trazabilidad, en aras de garantizar su privacidad.

Remarcar que los dos primeros requisitos son antagónicos, es decir, si deseamos proveer anonimato no es trivial proveer autenticación y viceversa.

Otros requisitos adicionales deseables serían la resistencia a ataques de denegación de servicio (seguridad), evitar la trazabilidad hacia atrás (*backward untraceability)* (privacidad), evitar la trazabilidad hacia delante (*forward untraceability).*

Para concluir con los requisitos, en la práctica son deseables la eficiencia computacional y de uso de memoria (rendimiento) y la escalabilidad (rendimiento).

Indicar también, que algunas de estas características son contradictorias entre sí, y por tanto se deberá ponderar para cada protocolo cuál es más necesaria. Ejemplos de estas contradicciones son por ejemplo seguridad - rendimiento (la eficiencia se consigue sacrificando el nivel de seguridad), privacidad - escalabilidad o privacidad – escalabilidad – eficiencia computacional.

Hay que tener en cuenta que, como se ha señalado, uno de los principales problemas que deben resolver estos protocolos es cumplir con los requisitos de seguridad manteniendo el anonimato e impidiendo la trazabilidad, aspectos que como se ha mencionado anteriormente, no se necesitan en el sistema que se está presentando.

A continuación se citan brevemente algunos de los protocolos propuestos para la autenticación en criptografía ligera, con la clasificación propuesta por [CHAI2012]:

- **Protocolos orientados a la escalabilidad**:
  - Molnar y Wagner [MOLNAR2004] propusieron un esquema de árbol basado en el trabajo de Weis [WEIS2003].
  - Burmester y otros presentaron un sistema de autenticación anónima [BURMESTER2008], que es una de las soluciones que preservan la privacidad más escalable. La autenticación anónima permite la concesión de ciertos privilegios o permisos sin preguntar el nombre de usuario o la contraseña. Un ejemplo típico en el ámbito de una red de computadores sería el acceso a las áreas públicas de un sitio web o un servidor FTP.
  - Cheon, Hong y Tsudik, mostraron una interesante idea para reducir la carga del lector: el uso de una estrategia *meet-in-the-middle* [CHEON2012].

- **Protocolos orientados a evitar la trazabilidad hacia atrás** (*Backward Untreaceability)*:

- Protocolo RFID escalable y probabilísticamente seguro basado en *hash*, de Avoine y Oechslin [AVOINE2005].
- YA-TRAP permite evitar la trazabilidad incluso cuando la etiqueta ha sido comprometida [TSUDIK2006]. Es vulnerable a ataques DoS tanto en la base de datos como en la etiqueta.
- O-TRAP [BURMESTER2006], solventa los problemas del anterior. Está basado en un esquema de cadena de *hash*.
- RIPP-FS [CONTI2007] pretende ofrecer más seguridad que los dos anteriores, aunque también se le descubrió una vulnerabilidad.

Todos los anteriores están basados en el uso de funciones de *hash* que debe realizar la etiqueta, lo que hace que requieran etiquetas de coste elevado. En 2010 Billet, Ettrong y Gilbert propusieron un protocolo ligero de autenticación mutua usando un cifrador de flujo [BILLET2010], que aportaba seguridad, eficiencia y una gran privacidad respecto a evitar la trazabilidad hacia atrás.

- **Protocolos orientados a evitar la trazabilidad hacia adelante** (*Forward Untreaceability)*:
  - En [LIM2006] Lim y Kwon proponen un esquema que cumple la evitación de la trazabilidad tanto hacia delante como hacia atrás. También es seguro contra la suplantación de servidores y los ataques DoS, siendo su principal inconveniente que no es escalable. En 2011 se presentó un método para romper la evitación de la trazabilidad [SAFKHANI2011].
  - Song y Mitchell [SONG2008] propusieron en 2008 unas mejoras al protocolo anterior.

- **Protocolos orientados al rendimiento:**
  - **Familia HB:** en el año 2005 Weiss [WEIS2005] presenta el concepto de autenticación hombre-máquina *(human-computer)* inspirado en los trabajos de Hopper y Blum [HOPPER2000]. La seguridad de estos protocolos se basa en el problema del aprendizaje de paridad con ruido (*Learning Parity with Noisy problem,* LNP), el cual está relacionado con la dificultad de decodificar un código lineal aleatorio.

- Protocolo HB [HOPPER2000, HOPPER2001]: proporciona seguridad frente a ataques pasivos (*eavesdropping).*
- Protocolo HB+ [JUELS2006]: proporciona seguridad contra algunos tipos de adversarios activos. Es un protocolo de autenticación de clave simétrica multirronda, donde cada ronda consta de tres comunicaciones entre el lector y la etiqueta.

Sin embargo, Gilbert, Robshaw y Silbert plantearon un ataque de hombre en medio *(man-in-the-midle)*, conocido como GRS [GILBERT2005] que vulneraba el protocolo HB+. Surgieron nuevos protocolos supuestamente resistentes al ataque GRS como HB++ [BRINGER2006], HB* [DUC2007], HB-MP' y HB-MP [MUNILLA2007], aunque estos sí son vulnerables a ataques pasivos y por tanto menos seguros que HB+ [GILBERT2008a]). En [GILBERT2008a] Gilbert *et al.* demuestran que estas variantes de HB+ tampoco son seguras.

En esta línea de trabajo, surgen nuevos protocolos como:

- Protocolo HB# [GILBERT2008b] y Random-HB#: resistentes al ataque GRS en algunas circunstancias.

Y nuevos ataques como el OOV [OUAFI2008].

Posteriormente han surgido algunas alternativas como el protocolo LCMQ propuesto por Li *et al* en [LI2010], basado en un tipo especial de matriz circulante denominada *circulant-P2 matrix*, y utilizando también el problema del aprendizaje de paridad con ruido (LPN) y el problema de multivariables cuadráticas.

- **Familia EPC-Gen2:** las etiquetas RFID EPC-Gen2 fueron diseñadas buscando un compromiso entre funcionalidad y coste, con poca atención a la seguridad [CHAI2012]. Para solucionar el tema de las seguridad se han propuesto diferentes protocolos, entre los que destacan [CHEN2009a], [CAI2008] (ambos

vulnerables a ataques de trazabilidad y repetición, Gen2+ [SUN2009] y [BLASS2011].

- **Otros protocolos:**

  Dentro de esta categoría podemos encontrar protocolos de autenticación que no encajan en ninguna de las categorías anteriores, como:

  - **Enyuntado de prueba** *(yoking proof)*: aunque la traducción suena un poco extraña, el concepto es muy gráfico, propuesto en [JUELS2004] por Juels, está basado en que para la autenticación se precisa que existan dos etiquetas determinadas en el rango de comunicación (lo que presupone que se encuentran unidas), por ejemplo un producto y su precinto de seguridad. Diversos trabajos han seguido esta línea de autenticación [BOLOTNYY2006, CHIEN2009, CHIEN2011, CHO2008].

  - **Protocolo *Adopted-Pet*:** descrito en [AMARIUCAI2012], es un protocolo automático de emparejamiento seguro (*secure pairing)*, este protocolo se basa en el tiempo de comunicación ininterrumpida entre el lector legítimo y una etiqueta legítima suficientemente cercanos.

  - **Protocolos de transferencia de propiedad** *(ownership transfer protocols)***:** permiten que las etiquetas cambien de propietario (es decir, quien puede acceder a ellas). Ejemplos: [CHEN2009b, KAPOOR2012, KORALALAGE2007, MOLNAR2005, SONG2011]

Comentar que hay algunas implementaciones de seguridad, que también ofrecen autenticación, basada en la capa física, es decir tanto en la propia comunicación de la tarjeta como en la forma de comunicarse. Se van a citar brevemente algunos de los más importantes:

- **Protocolos de distancia definida** *(Distance Bounding Protocols):* diseñados para combatir algunos tipos de ataque como el "Engaño de Mafia" (*Mafia Fraud)* , el engaño de distancia *(Distance Fraud)* o el ataque terrorista (*Terrorist Attack)*. Están basados en la suposición de

que un lector legítimo dentro de una distancia definida tendrá un tiempo de procesado y propagación de la señal corto y constante.

- **Protocolo de Hancke y Kuh** [HANCKE2005]**:** basado en primer protocolo de distancia definida propuesto por Brands and Chaum [BRANDS1994], eliminando la última fase del proceso y adaptándolo para su aplicación en sistemas RFID.
- **Protocolo de Kim y Avoine** [KIM2009a]**:** basado en el anterior, introdujeron algunas mejoras.
- **Peris *et al.*** [PERIS-LOPEZ2010]**:** basado en el concepto de protección contra inundación utilizado en sistemas anti-spam o TCP-SYN, pero aplicado a RFID.

Otros: otros trabajos en esta línea son [AVOINE2009, DÜRHOLZ2011, KAPOOR2008, KARA2010, KARDAŞ2012, KIM2009b, MUNILLA2008, ONAT2009, PERIS-LOPEZ2011]

Anexo IV. Normativa de trazabilidad y seguridad alimentaria.

1. Reglamento (CE) nº 178/2002 del Parlamento Europeo y del Consejo de 28 de enero de 2002 por el que se establecen los principios y los requisitos generales de la legislación alimentaria, se crea la Autoridad Europea de Seguridad Alimentaria y se fijan procedimientos relativos a la seguridad alimentaria (D.O.C.E: nº L31 de 1.2.2002).

El **artículo 18** de la citada disposición establece por primera vez, con carácter horizontal, para todas las empresas alimentarias y de piensos que forman parte de la cadena alimentaría la obligación de poner en marcha, aplicar y mantener un sistema de trazabilidad. Dicho artículo es aplicable desde el 1 de enero de 2005.

"Artículo 18. Trazabilidad

1. *En todas las etapas de la producción, la transformación y la distribución deberá asegurarse la trazabilidad de los alimentos, los piensos, los animales destinados a la producción de alimentos y de cualquier otra sustancia destinada a ser incorporada en un alimento o un pienso, o con probabilidad de serlo.*
2. *Los operadores económicos de empresas alimentarias y de empresas de piensos deberán poder identificar a cualquier persona que les haya suministrado un alimento, un pienso, un animal destinado a la producción de alimentos, o cualquier sustancia destinada a ser incorporada en un alimento o un pienso, o con probabilidad de serlo. Para tal fin, dichos operadores económicos pondrán en práctica sistemas y procedimientos que permitan poner esta información a disposición de las autoridades competentes si éstas así lo solicitan.*
3. *Los operadores económicos de empresas alimentarias y de empresas de piensos deberán poner en práctica sistemas y procedimientos para identificar a las empresas a las que hayan suministrado sus productos. Pondrán esta información a disposición de las autoridades competentes si éstas así lo solicitan.*
4. *Los alimentos o los piensos comercializados o con probabilidad de comercializarse en la Comunidad deberán estar adecuadamente etiquetados o identificados para facilitar su trazabilidad mediante documentación o información pertinentes, de acuerdo con los requisitos pertinentes de disposiciones más específicas.*

5. Podrán adoptarse disposiciones para la aplicación de lo dispuesto en el presente artículo en relación con sectores específicos de acuerdo con el procedimiento contemplado en el apartado 2 del artículo 58."

Los sistemas que se desarrollen, consecuencia de lo establecido en dicho artículo, deberán cumplir los mismos objetivos del Reglamento 178/2002, del que forman parte:

- Lograr un nivel elevado de protección de la vida y la salud de las personas,
- Proteger los intereses de los consumidores, incluidas unas prácticas justas en el comercio de alimentos
- Evitar:
    - las prácticas fraudulentas o engañosas;
    - la adulteración de alimentos, y
    - cualquier otra práctica que pueda inducir a engaño al consumidor.

El **artículo 19** establece las responsabilidades respecto a los alimentos de los operadores económicos de empresas alimentarias consistentes en la comunicación y participación de los operadores de la cadena alimentaria cuando se detecte que algún alimento no cumple los requisitos de seguridad. Se establecerá una comunicación tanto con los consumidores (si el producto ha llegado a ellos) como con las autoridades competentes. También se establece la obligación por parte del operador de la retirada del producto.

El **artículo 20** dispone las mismas responsabilidades para el operador económico de empresa de piensos.

***2.* Libro Blanco sobre la Seguridad alimentaria.** La Comisión Europea perfiló una revisión radical de las normas de higiene y seguridad alimentaria de la Comunidad, conforme a las cuales, los operadores de empresa alimentaria son los principales responsables de la seguridad alimentaria. La innovación principal de este conjunto de Reglamentos y Directivas aplicables desde el 1 de enero de 2006, es la realización de una política de higiene única, transparente y aplicable a todos los alimentos y todos los operadores de alimentos que intervienen de la granja a la mesa, junto con la introducción de instrumentos eficaces para gestionar la seguridad alimentaria y cualquier crisis alimentaria en todas las etapas de la cadena de alimentos. De dos de estos Reglamentos se pueden extraer algunas de las

disposiciones más importantes que contribuyen o facilitan el procedimiento de trazabilidad.

3. Reglamento (CE) Nº 852/2004 del Parlamento europeo y del Consejo de 29 de abril de 2004 relativo a la higiene de los productos alimenticios (H1) (D.O.C.E: nº L 226 de 25.6.2004).

En el **artículo 5** se establece la obligación para los operadores de empresa alimentaria que intervengan en cualquier etapa de la producción, transformación y distribución de alimentos posteriores a la producción primaria de crear, aplicar y mantener un procedimiento o procedimientos permanentes basados en los principios del APPCC. Dicho sistema implica la elaboración de documentos y registros en función de la naturaleza y el tamaño de la empresa alimentaria para demostrar su aplicación efectiva, que pueden contribuir a la información necesaria del sistema de trazabilidad.

"Artículo 5. Sistema de análisis de peligros y puntos de control crítico.

1. *Los operadores de empresa alimentaria deberán crear, aplicar y mantener un procedimiento o procedimientos permanentes basados en los principios del APPCC.*
2. *Los principios APPCC son los siguientes:*

   a) detectar cualquier peligro que deba evitarse, eliminarse o reducirse a niveles aceptables;

   b) detectar los puntos de control crítico en la fase o fases en las que el control sea esencial para evitar o eliminar un peligro o reducirlo a niveles aceptables;

   c) establecer, en los puntos de control crítico, límites críticos que diferencien la aceptabilidad de la inaceptabilidad para la prevención, eliminación o reducción de los peligros detectados;

   d) establecer y aplicar procedimientos de vigilancia efectivos en los puntos de control crítico;

   e) establecer medidas correctivas cuando la vigilancia indique que un punto de control crítico no está controlado;

   f) establecer procedimientos, que se aplicarán regularmente, para verificar que las medidas contempladas en las letras a) a e) son eficaces; y

   g) elaborar documentos y registros en función de la naturaleza y el tamaño de la empresa alimentaria para demostrar la aplicación efectiva de las medidas contempladas en las letras a) a f)."

En la Parte A del anexo 1, se indican una serie de Registros que son obligatorios para la producción primaria y que pueden contribuir a la información necesaria del sistema de trazabilidad:

> *"7. Los operadores de la empresa alimentaria deberán llevar y conservar registros sobre las medidas aplicadas para controlar los peligros de manera adecuada y durante un período adecuado teniendo en cuenta la naturaleza y el tamaño de la empresa alimentaria. Previa petición, los operadores de empresa alimentaria pondrán la información relevante que conste en dichos registros a disposición de las autoridades competentes y de los operadores de empresa alimentaria de recepción.*
>
> *8. Los operadores de empresa alimentaria que críen animales o que produzcan productos primarios de origen animal deberán, en particular, llevar registros sobre:*
>
> *a) la naturaleza y el origen de los alimentos suministrados a los animales;*
>
> *b) el detalle de los medicamentos veterinarios u otros tratamientos administrados a los animales, las fechas de su administración y los tiempos de espera;*
>
> *c) la aparición de enfermedades que puedan afectar a la seguridad de los productos de origen animal;*
>
> *d) los resultados de todos los análisis efectuados en muestras tomadas de animales y otras muestras tomadas con fines de diagnóstico, que tengan importancia para la salud humana; y*
>
> *e) todos los informes pertinentes sobre los controles efectuados a animales o a productos de origen animal.*
>
> *9. Los operadores de empresa alimentaria que produzcan o cosechen productos vegetales deberán, en particular, llevar registros sobre:*
>
> *a) la utilización de productos fitosanitarios y biocidas;*
>
> *b) la aparición de plagas o de enfermedades que puedan afectar a la seguridad de los productos de origen vegetal; y*
>
> *c) los resultados de todos los análisis pertinentes efectuados en muestras tomadas de plantas u otras muestras que tengan importancia para la salud humana."*

En el capítulo II de este Reglamento, está previsto que los Estados miembros fomenten la elaboración de guías nacionales de prácticas correctas de higiene (GPCH) para la aplicación de los principios del sistema APPCC.

Se establece un procedimiento general para la elaboración de las GPCH y, por la idiosincrasia especial de la producción primaria que, además, se inicia como sector afectado en las regulaciones sobre higiene de los productos alimenticios, el Anexo 1, en su parte B da unas Recomendaciones para las guías destinadas a este sector, haciendo unas referencias concretas a la trazabilidad:

"2. Las guías de prácticas correctas de higiene deberán incluir la oportuna información sobre los peligros que puedan presentarse en la producción primaria y operaciones conexas, así como las medidas para combatirlos, incluidas las medidas correspondientes establecidas en la legislación comunitaria y nacional y en los programas nacionales y comunitarios. Entre los ejemplos de estos peligros y medidas pueden incluirse: [...]

c) el uso correcto y adecuado de productos fitosanitarios y biocidas, y su trazabilidad;

d) el uso correcto y adecuado de medicamentos veterinarios y aditivos alimentarios y su trazabilidad;

e) la preparación, el almacenamiento, la utilización y la trazabilidad de los piensos".

4. Reglamento (CE) no 853/2004 del Parlamento europeo y del Consejo de 29 de abril de 2004 por el que se establecen normas específicas de higiene de los alimentos de origen animal (H2) (D.O.C.E. nº L 226 de 25.6.2004).

Además de cumplir las normas generales del Reglamento (CE) nº 178/2002, los operadores de empresa alimentaria responsables de los establecimientos sujetos a autorización con arreglo al presente Reglamento deben asegurarse de que todos los productos de origen animal que pongan en el mercado llevan una marca sanitaria o una marca de identificación.

5. Reglamento (CE) nº 183/2005 del Parlamento europeo y del Consejo de 12 de enero de 2005 por el que se fijan requisitos en materia de higiene de los piensos (D.O.C.E. L 35 de 8.2.2005).

El artículo 6 del Reglamento por el que se fijan requisitos en materia de higiene de los piensos establece que:

"Los explotadores de empresas de piensos que no intervengan en la producción primaria de piensos deberán poner a punto, aplicar y mantener uno o varios procedimientos permanentes basados en los principios del sistema HACCP (análisis de peligros y puntos de control crítico)".

6. Real Decreto 1808/1991, de 13 de diciembre, que regula las menciones o marcas que permiten identificar el lote al que pertenece un producto alimenticio (BOE 25.12.1991).

Resultado de la transposición de la Directiva del Consejo 89/396/CEE, de 14 de junio de 1989, esta legislación requiere una indicación o marca de identificación del lote al que pertenece el alimento.

Además de las normas citadas, basadas en la información contenida en [AESAN2009], para el caso que nos ocupa, existe además legislación propia de la comunidad autónoma donde se lleva a cabo la actividad de producción, en este caso Aragón, y que se cita a continuación:

- **Ley 9/2006, de 30 de noviembre, de Calidad Alimentaria en Aragón** ("Boletín Oficial de Aragón" nº 142, de 13 de diciembre de 2006).
- **Decreto 5/2009, de 13 de enero, del Gobierno de Aragón**, por el que se aprueba el Reglamento del contenido mínimo de la normativa específica de determinadas denominaciones geográficas de calidad de los alimentos y el procedimiento para su reconocimiento ("Boletín Oficial de Aragón" nº 18, de 28 de enero de 2009).

Bibliografía

Abawajy, J. 2009, "Enhancing RFID Tag Resistance against Cloning Attack", *Network and System Security, 2009. NSS '09. Third International Conference on*, pp. 18.

Abdul-Rahman, A. & Hailes, S. 2000, "Supporting trust in virtual communities", *The 33rd Annual Hawaii International Conference on System Sciences (HICSS-33)*IEEE, Los Alamitos, CA, United States, 4 January 2000 through 7 January 2000, pp. 132.

ACSQHC, Australian Commission on Safety and Quality in Health Care 2010, *Architecture and Technical Standards for Australian Clinical Quality Registries*, Sydney.

AESAN 2009, *Guia para la aplicacion del sistema de trazabilidad en la empresa agroalimentaria. Agencia Española de Seguridad Alimentaria y Nutrición*.

Ahn, G. & Ko, M. 2007, "User-centric privacy management for federated identity management", *Proceedings of the 3rd International Conference on Collaborative Computing: Networking, Applications and Worksharing, CollaborateCom 2007*, pp. 187.

Alañón, M.E., Díaz-Maroto, M.C., Díaz-Maroto, I.J., Vila-Lameiro, P. & Pérez-Coello, M.S. 2011, "Cyclic Polyalcohols: Fingerprints to Identify the Botanical Origin of Natural Woods Used in Wine Aging", *Journal of Agricultural and Food Chemistry,* vol. 59, no. 4, pp. 1269-1274.

Albersmeier, F., Schulze, H., Jahn, G. & Spiller, A. 2009, "The reliability of third-party certification in the food chain: From checklists to risk-oriented auditing", *Food Control,* vol. 20, no. 10, pp. 927-935.

Amariucai, G.T., Bergman, C. & Guan, Y. 2012, *An automatic, time-based, secure pairing protocol for passive RFID*, Amherst, MA edn.

Anderson, R. 2008, *Security engineering: a guide to building dependable distributed systems,* 2nd edn, Wiley Pub., Indianapolis, IN.

Angeles, R. 2005, "RFID technologies: Supply-chain applications and implementation issues", *Information Systems Management,* vol. 22, no. 1, pp. 51-65.

Arienzo, A., Coff, C. & Barling, D. 2008, "The European Union and the regulation of food traceability: from risk management to informed choice?", *Ethical Traceability and Communicating Food,* , pp. 23-41.

Atici, A.C., Fan, J., Batina, L., Verbauwhede, I. & Yalçin, S.B.Ö. 2008, "Low-cost Implementations of NTRU for pervasive security", *ASAP08 - IEEE 19th International Conference on Application-Specific Systems, Architectures and Processors*, 2 July 2008 through 4 July 2008, pp. 79.

Auto-ID Center 2003a, *13.56 MHz ISM Band Class 1 Radio Frequency (RF) Identification Tag Interface Specification defines communications interface and protocol, RF, and tag requirements.*

Auto-ID Center 2003b, *860MHz -- 930 MHz Class 1 Radio Frequency (RF) Identification Tag Radio Frequency & Logical Communication Interface Specification defines communications interface and protocol, RF, and tag requirements.*

Auto-ID Center 2003c, *900 MHz Class 0 Radio Frequency (RF) Identification Tag Specification communications interface and protocol, RF, and tag requirements, operational algorithms for 900MHz communications.*

Avoine, G. & Oechslin, P. 2005, "A scalable and provably secure hash-based RFID protocol", *Third IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom 2005 Workshops*, 8 March 2005 through 12 March 2005, pp. 110.

Avoine, G. & Tchamkerten, A. 2009, *An efficient distance bounding rfid authentication protocol: Balancing false-acceptance rate and memory requirement*, Pisa edn.

Avoine, G. & Oechslin, P. 2005, "RFID Traceability: A Multilayer Problem", *The 9th International Conference on Financial Cryptography - FC'05*, pp. 125.

Ayoade, J. 2007, "Roadmap to solving security and privacy concerns in RFID systems", *Computer Law & Security Report,* vol. 23, no. 6, pp. 555-561.

Balke, T., Knig, S. & Torsten, E. 2009, *A Survey on Reputation Systems for Artificial Societies,* Universitätsbibliothek Bayreuth, Bayreuth.

Banks, J., Pachano, M.A., Thompson, L.G. & Hanny, D. 2007, *RFID Applied,* Wiley, Hoboken, New Yersey.

Banterle, A. & Stranieri, S. 2008, "The consequences of voluntary traceability system for supply chain relationships. An application of transaction cost economics", *Food Policy,* vol. 33, no. 6, pp. 560-569.

Barjis, J. & Samuel, F.W. 2010, "Organizational and business impacts of RFID technology", *Business Process Management Journal,* vol. 16, no. 6, pp. 897-903.

Becerra, G., Heard, J., Kremer, R. & Denzinger, J. 2007, "Trust Attributes, Methods, and Uses ", *Tenth Workshop on Trust in Agent Societies*, eds. R. Falcone, S. Barber, J. Sabater-Mir & M. Singh, , Mayo 2007, pp. 1.

Bertino, E., Paci, F. & Shang, N. 2009, "Digital identity protection- Concepts and issues", *4th International Conference on Availability, Reliability and Security, ARES 2009 , art. no. 5066445 , pp. lxix-lxxviii.*

Billet, O., Etrog, J. & Gilbert, H. 2010, "Lightweight privacy preserving authentication for RFID using a stream cipher", *17th International Workshop on Fast Software Encryption, FSE 2010,Seoul* , Vol. 6147 LNCS, 2010, Pages 55-74.

Blass, E.-., Kurmus, A., Molva, R., Noubir, G. & Shikfa, A. 2011, "The Ff-family of protocols for RFID-privacy and authentication", *IEEE Transactions on Dependable and Secure Computing,* vol. 8, no. 3, pp. 466-480.

Bolan, C. 2006, "The Lazarus Effect: Resurrecting Killed RFID Tags", *Proceedings of the 4th Australian Information Security Management Conference.*

Boldyreva, A. 2002, *Threshold signatures, multisignatures and blind signatures based on the Gap-Diffie-Hellman-group signature scheme*, Volume 2567, 2002, pp. 31-46.

Bolotnyy, L. & Robins, G. 2006, "Generalized "yoking-proofs" for a group of RFID tags", *2006 3rd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, MobiQuitous*, 17 July 2006 through 21 July 2006.

Bolotnyy, L. & Robins, G. 2007, "Physically Unclonable Function-Based Security and Privacy in RFID Systems", *Pervasive Computing and Communications, 2007. PerCom '07. Fifth Annual IEEE International Conference on*, pp. 211.

Boneh, D., Lynn, B. & Shacham, H. 2001, "Short signatures from the Weil pairing", *Proceedings og Asiacrypt 2001*, ed. 480, Springer-Verlag, , 2001, pp. 465.

Boneh, D., Lynn, B. & Shacham, H. 2004, "Short signatures from the weil pairing", *Journal of Cryptology,* vol. 17, no. 4, pp. 297-319.

Boneh, D., Gentry, C., Lynn, B. & Shacham, H. 2003, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps" in *Advances in Cryptology — EUROCRYPT 2003*, ed. E. Biham, Springer Berlin / Heidelberg, , pp. 416-432.

Bottani, E. & Rizzi, A. 2008, "Economical assessment of the impact of RFID technology and EPC system on the fast-moving consumer goods supply chain", *International Journal of Production Economics,* vol. 112, no. 2, pp. 548-569.

Boursas, L. & Danciu, V.A. 2008, "Dynamic inter-organizational cooperation setup in Circle-of-Trust environments", *NOMS 2008 - IEEE/IFIP Network Operations and Management Symposium: Pervasive Management for Ubiquitous Networks and Services*, 7 April 2008 through 11 April 2008, pp. 113.

Brands, S. & Chaum, D. 1994, "Distance-bounding protocols", *Lecture Notes in Computer Science,* vol. 765, pp. 344-359.

Bringer, J., Chabanne, H. & Dottax, E. 2006, "HB++: A lightweight authentication protocol secure against some attacks", *Proceedings - Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, SecPerU 2006*, pp. 28.

Bromley, D.B. 1993, Reputation, Image and Impression Management, Ed. Wiley; 1st edition (May 1993).

Buhr, B.L. 2003, "Traceability and information technology in the meat supply chain: Implications for firm organization and market structure", *Journal of Food Distribution Research,* vol. 34, no. 3, pp. 13-26.

Bullock, D.S., Desquilbet, M. & Nitsi, E.I. 2000, " The Economics of Non-GMO Segregation and Identity Preservation". Department of Agricultural and Consumer Economics. University of Illinois at Urbana - Champaign, November 2000.

Burmester, M., De Medeiros, B. & Motta, R. 2008, "Robust, anonymous RFID authentication with constant key-lookup", *2008 ACM Symposium on Information, Computer and Communications Security, ASIACCS '08*, 18 March 2008 through 20 March 2008, pp. 283.

Burmester, M., Van Le, T. & De Medeiros, B. 2006, "Provably secure ubiquitous systems: Universally composable RFID authentication protocols", *2006 Securecomm and Workshops*, 28 August 2006 through 1 September 2006.

Buskens, V. 1998, "The social structure of trust", *Social Networks,* vol. 20, no. 3, pp. 265-289.

Caballero, A. 2008, *Definición de un modelo de gestión de las nociones de confianza y reputación entre agentes. Enfoque basado en la similitud entre tareas.*, Universidad de Murcia. Departamento de Ingeniería de la Información y las Comunicaciones.

Caballero, A., Garcia-Valverde, T., Botia, J.A. & Gomez-Skarmeta, A. 2009, "A trust and reputation model as adaptive mechanism for multi-agent systems", *Inteligencia Artificial,* vol. 13, no. 42, pp. 3-11.

Cai, Q., Zhan, Y. & Wang, Y. 2008, "A minimalist mutual authentication protocol for RFID system & BAN logic analysis", *ISECS International Colloquium on Computing, Communication, Control, and Management, CCCM 2008*, 3 August 2008 through 4 August 2008, pp. 449.

Camp, J.L. 2004, "Digital identity", *Technology and Society Magazine, IEEE,* vol. 23, no. 3, pp. 34-41.

Canavari, M., Centonze, R., Hingley, M. & Spadoni, R. 2010, "Traceability as part of competitive strategy in the fruit supply chain", *British Food Journal,* vol. 112, no. 2, pp. 171-186.

Cao, Y. & Yang, L. 2010, "A survey of Identity Management technology", *2010 IEEE International Conference on Information Theory and Information Security, ICITIS 2010*, 17 December 2010 through 19 December 2010, pp. 287.

Capitani, S., Foresti, S., Jajodia, S., Paraboschi, S. & Samarati, P. 2011, "Authorization enforcement in distributed query evaluation", *Journal of Computer Security,* vol. 19, no. 4, pp. 751-794.

Carbo, J., Molina, J.M. & Davila, J. 2003, "Trust management through fuzzy reputation", *International Journal of Cooperative Information Systems,* vol. 12, no. 1, pp. 135-155.

Carriquiry, M. & Babcock, B.A. 2007, "Reputations, market structure, and the choice of quality assurance systems in the food industry", *American Journal of Agricultural Economics,* vol. 89, no. 1, pp. 12-23.

Carter, J., Bitting, E. & Ghorbani, A.A. 2002, "Reputation formalization for an information-sharing multi-agent system", *Computational Intelligence,* vol. 18, no. 4, pp. 515-534.

Castelfranchi, C. & Falcone, R. 1998, "Principles of trust for MAS: Cognitive anatomy, social importance, and quantification", *Proceedings of 3rd International Conference on MultiAgent Systems,* , pp. 72-79.

Castelfranchi, C. & Paglieri, F. 2007, "The role of beliefs in goal dynamics: Prolegomena to a constructive theory of intentions", *Synthese,* vol. 155, no. 2, pp. 237-263.

Celentani, M., Fudenberg, D., Levine, D.K. & Pesendorfer, W. 1996, "Maintaining a reputation against a long-lived opponent", *Econometrica,* vol. 64, no. 3, pp. 691-704.

Chai, Q. 2012, *Design and Analysis of Security Schemes for Low-Cost RFID Systems*, University of Waterloo.

Chang, J.L., Shen, C.X., Zhen, H., He, Y.Z. & Liu, Y. 2009, "Survey of research on identity management", *Computer Engineering and Design,* vol. 30, pp. 1365.

Chen, C. & Deng, Y. 2009a, "Conformation of EPC Class 1 Generation 2 standards RFID system with mutual authentication and privacy protection", *Engineering Applications of Artificial Intelligence,* vol. 22, no. 8, pp. 1284-1291.

Chen, H., Lee, W., Zhao, Y. & Chen, Y.-. 2009b, "Enhancement of the RFID security method with ownership transfer", *Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication, ICUIMC'09*, pp. 251.

Cheon, J.H., Hong, J. & Tsudik, G. 2012, "Reducing RFID reader load with the meet-in-the-middle strategy", *Journal of Communications and Networks,* vol. 14, no. 1, pp. 10-14.

Chien, H. & Liu, S. 2009, "Tree-based RFID yoking proof", *International Conference on Networks Security, Wireless Communications and Trusted Computing, NSWCTC 2009*, 25 April 2009 through 26 April 2009, pp. 550.

Chien, H., Yeh, M., Wu, T. & Lee, C. 2011, "Comments on enhanced yoking proof protocols for radio frequency identification tags and tag groups", *Journal of Shanghai Jiaotong University (Science),* vol. 16, no. 5, pp. 604-609.

Cho, J., Yeo, S., Hwang, S., Rhee, S. & Kim, S.K. 2008, "Enhanced yoking proof protocols for RFID tags and tag groups", *22nd International Conference on Advanced Information Networking and Applications Workshops/Symposia, AINA 2008*, 25 March 2008 through 28 March 2008, pp. 1591.

Chryssochoidis, G., Karagiannaki, A., Pramatari, K. & Kehagia, O. 2009, "A cost-benefit evaluation framework of an electronic-based traceability system", *British Food Journal,* vol. 111, no. 6, pp. 565-582.

Clarke, J. 2009a, "Code-Level Defenses" in *SQL Injection Attacks and Defense* Syngress, Boston, pp. 341-376.

Clarke, J. 2009b, "Platform-Level Defenses" in *SQL Injection Attacks and Defense* Syngress, Boston, pp. 377-413.

Coff, C., Korthals, M. & Barling, D. 2008, "Ethical traceability and informed food choice", *Ethical Traceability and Communicating Food,* pp. 1-18.

Conte, R. & Paolucci, M. 2002, *Reputation in artificial societies: social beliefs for social order,* Kluwer Academic Publishers, Boston.

Conti, M., Di Pietro, R., Mancini, L.V. & Spognardi, A. 2007, "RIPP-FS: An RFID identification, privacy preserving protocol with forward secrecy", *5th*

Annual IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2007, 19 March 2007 through 23 March 2007, pp. 229.

Cranor, L.F. & Garfinkel, S. 2005, *Security and usability: designing secure systems that people can use,* O'Reilly, Beijing ; Sebastapol, CA.

Dabrowski, M. & Pacyna, P. 2008, "Generic and complete three-level identity management model", *2nd International Conference on Emerging Security Information, Systems and Technologies.*

Damiani, E., De Capitani di Vimercati, S. & Samarati, P. 2003, "Managing Multiple and Dependable Identities", *IEEE Internet Computing,* vol. 7, no. 6, pp. 29-37.

David, M. 2011, *Lightweight Cryptography for Passive RFID Tags,* Aalborg University, Dinamarca.

de Jonge, J., van Trijp, H., Goddard, E. & Frewer, L. 2008, "Consumer confidence in the safety of food in Canada and the Netherlands: The validation of a generic framework", *Food Quality and Preference,* vol. 19, no. 5, pp. 439-451.

Deimel, M., Frentrup, M. & Theuvsen, L. 2008, "Transparency in food supply chains: Empirical results from German pig and dairy production", *Journal on Chain and Network Science,* vol. 8, no. 1, pp. 21-32.

Devadas, S., Suh, E., Paral, S., Sowell, R., Ziola, T. & Khandelwal, V. 2008, "Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications", *RFID, 2008 IEEE International Conference on*, pp. 58.

Dickinson, D.L. & Bailey, D. 2005, "Experimental evidence on willingness to pay for red meat traceability in the United States, Canada, the United Kingdom, and Japan", *Journal of Agricultural and Applied Economics,* vol. 37, no. 3, pp. 537-548.

Duc, D.N. & Kim, K. 2007, "Securing HB Against GRS Man-in-the-Middle Attack+", *Institute of Electronics, Information and Communication Engineers, Symposium on Cryptography and Information Security,* pp. 23-26.

Duc, D.N., Park, J., Lee, H. & Kim, K. 2006, "Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning", *Proc. of SCIS 2006,* pp. 97.

Dürholz, U., Fischlin, M., Kasper, M. & Onete, C. 2011, *A formal approach to distance-bounding RFID protocols*, Xi'an edn.

Economics, F. 2011, *Estimating the global economic and social impacts of counterfeiting and piracy*, FRONTIER ECONOMICS EUROPE.

Eisenbarth, T., Kumar, S., Paar, C., Poschmann, A. & Uhsadel, L. 2007, "A survey of lightweight-cryptography implementations", *IEEE Design and Test of Computers,* vol. 24, no. 6, pp. 522-533.

El-Haleem, A.M.A., Ali, I.A., Ibrahim, I.I. & El-Sawy, A.R.H. 2010, "Trust model for TRIDNT trust based routing Protocol", *Computer Technology and Development (ICCTD), 2010 2nd International Conference on*, pp. 538.

El-Said, M.M. & Woodring, I. 2009, "An Empirical Study for Protecting Passive RFID Systems against Cloning", *Information Technology: New Generations, 2009. ITNG '09. Sixth International Conference on*, pp. 558.

Esfandiari, B. & Chandrasekharan, S. 2001, "On how agents make friends: Mechanisms for trust acquisition", *Proceedings of the Fifth International Conference on Autonomous Agents Workshop on Deception, Fraud and Trust in Agent Societies,* pp. 27-34.

European Parliament 2002, *Regulation (EC) No. 178/2002 of the European Parliament and of the Council.*

Fayolle, L., Lépine, T., Fournel, T. & Boutant, Y. 2008, "Deflectometry for secure traceability", *Journal of Physics: Conference Series,* vol. 139.

Ferraiolo, D. & Kuhn, R. 1992, "Role-based access controls", *15th National Computer Security Conference,* pp. 554-563.

Flynn, A., Marsden, T.T. & Smith, E. 2003, "Food Regulation and Retailing in a New Institutional Context", *Political Quarterly,* vol. 74, no. 1, pp. 38-46+141.

Fritz, M. & Fischer, C. 2007, "The role of trust in European food chains: Theory and empirical findings", *International Food and Agribusiness Management Review,* vol. 10, no. 2, pp. 141-161.

Fuchs, L., Pernul, G. & Sandhu, R. 2011, "Roles in information security – A survey and classification of the research area", *Computers & Security,* vol. 30, no. 8, pp. 748-769.

Gambetta, D. 1988, *Trust: making and breaking cooperative relations,* B. Blackwell, New York, NY, USA.

Garfinkel, S.L., Juels, A. & Pappu, R. 2005, "RFID privacy: an overview of problems and proposed solutions", *Security & Privacy, IEEE,* vol. 3, no. 3, pp. 34-43.

Gellynck, X., Januszewska, R., Verbeke, W. & Viaene, J. 2007, "Firm's costs of traceability confronted with consumer requirements", *Quality Management in Food Chains,* pp. 45-56.

Gilbert, H., Robshaw, M. & Sibert, H. 2005, "Active attack against HB+: A provably secure lightweight authentication protocol", *Electronics Letters,* vol. 41, no. 21, pp. 1169-1170.

Gilbert, H., Robshaw, M.J.B. & Seurin, Y. 2008a, *Good variants of HB+ are hard to find*, Cozumel edn.

Gilbert, H., Robshaw, M.J.B. & Seurin, Y. 2008b, *HB#: Increasing the security and efficiency of HB+*, Istanbul edn.

Glover, B. & Bhatt, H. 2006, *RFID Essentials (Theory in Practice),* O'Reilly Media, Inc.

Golan, E., Krissoff, B., Kuchler, F., Nelson, K. & Price, G. 2004.

Gonzalez, J, García, I. & Fiestras, G. 2010, *An Introductory Course on Mathematical Game Theory*, Graduate Studies in Mathematics, 115, Ed. American Mathematical Society & Real Sociedad Matemática Española.

Gonzalez, J.M., Anwar, M. & Joshi, J.B.D. 2011, "Trust-Based Approaches to Solve Routing Issues in Ad-Hoc Wireless Networks: A Survey", *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on*, pp. 556.

GS1, 2012, *, Sitio Web del GS1*. Available: http://www.gs1.org/ [2012].

Hancke, G.P. & Kuhn, M.G. 2005, "An RFID distance bounding protocol", *1st International Conference on Security and Privacy for Emerging Areas in Communications Networks, SecureComm 2005*, 5 September 2005 through 9 September 2005, pp. 67.

Hanf, J. & Hanf, C.-. 2007, "Does food quality create a competitive advantage?", *Quality management in food chains,* , pp. 489-499.

He, W., Zhang, N., Tan, P.S., Lee, E.W., Li, T.Y. & Lim, T.L. 2008, "A secure RFID-based track and trace solution in supply chains", *IEEE INDIN 2008: 6th IEEE International Conference on Industrial Informatics*, 13 July 2008 through 16 July 2008, pp. 1364.

Herzig, A. 2010, *, ForTrust: social trust analysis and formalization,*. Avaible: http://www.irit.fr/ForTrust/ [Consultado 2011] .

Herzig, A., Lorini, E., Hübner, J.F., Ben-Naim, J., Boissier, O., Castelfranchi, C., Demolombe, R., Longin, D., Perrussel, L. & Vercouter, L. 2008, "Prolegomena for a logic of trust and reputation", *Third International Workshop on Normative Multiagent Systems*, Proceedings, pp. 143-157.

Heyder, M., Theuvsen, L. & Hollmann-Hespos, T. 2012a, "Investments in tracking and tracing systems in the food industry: A PLS analysis", *Food Policy,* vol. 37, no. 1, pp. 102-113.

Hobbs, J.E., Von Bailey, D., Dickinson, D.L. & Haghiri, M. 2005, "Traceability in the Canadian red meat sector: Do consumers care?", *Canadian Journal of Agricultural Economics,* vol. 53, no. 1, pp. 47-65.

Hobbs, J.E. 2004, "Information asymmetry and the role of traceability systems", *Agribusiness,* vol. 20, no. 4, pp. 397-415.

Hopper, N.J. & Blum, M. 2000, *A Secure Human-Computer Authentication Scheme.*

Hopper, N.J. & Blum, M. 2001, "Secure human identification protocols", *LNCS,* vol. 2248, pp. 52-66.

Huang, T.-., Yeh, Y. & Tzeng, D.D.S. 2011, "Barcode-like heteroduplex DNA pattern as an aid for rapid identification of anthracnose fungi", *New Biotechnology,* vol. 28, no. 1, pp. 72-78.

Hume, D. 1739, *A Treatise of Human Nature.*

Huynh, T.D., Jennings, N.R. & Shadbolt, N.R. 2006, "An integrated trust and reputation model for open multi-agent systems", *Autonomous Agents and Multi-Agent Systems,* vol. 13, no. 2, pp. 119-154.

Ilie-Zudor, E., Kemény, Z., Van Blommestein, F., Monostori, L. & Van Der Meulen, A. 2011, "A survey of applications and requirements of unique identification systems and RFID techniques", *Computers in Industry,* vol. 62, no. 3, pp. 227-252.

Itakura, K. & Nakamura, K. 1983, "PUBLIC-KEY CRYPTOSYSTEM SUITABLE FOR DIGITAL MULTISIGNATURES.", *NEC Research and Development,* , no. 71, pp. 1-8.

Jeng, A.B., Li-Chung Chang & Te-En Wei 2009, "Survey and remedy of the technologies used for RFID tags against counterfeiting", *Machine Learning and Cybernetics, 2009 International Conference on*, pp. 2975.

Cho, J., Swami, A. & I Chen, I. 2011, "A Survey on Trust Management for Mobile Ad Hoc Networks", *Communications Surveys & Tutorials, IEEE,* vol. 13, no. 4, pp. 562-583.

Jo, H., Lee, H., Chun, K. & Park, H. 2009, "Interoperability and anonymity for id management systems", *International Conference on Advanced Communication Technology, ICACT*, pp. 1257.

Jones, P., Clarke-Hill, C., Hillier, D., Shears, P. & Comfort, D. 2004, "Radio frequency identification in retailing and privacy and public policy issues", *Management Research News,* vol. 27, no. 8-9, pp. 46-56.

Jøsang, A. & Pope, S. 2005, "User centric identity management", *AusCERT Conference 2005, Proceedings of AusCERT Asia Pacific Information Technology Security Conference (AusCERT2005):* Refereed R&D Stream, Clark, A., Kerr, K., and Mohay, G. (Eds.), University of Queensland, 2005. ISBN: 1-86499-799-0, pp. 77-89.

Joshi, G.P. & Kim, S.W. 2008, "Survey, nomenclature and comparison of reader anti-collision protocols in RFID", *IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India),* vol. 25, no. 5, pp. 285-292.

Juels, A. 2004, ""Yoking-proofs" for RFID tags", *Proceedings - Second IEEE Annual Conference on Pervasive Computing and Communications, Workshops, PerCom 2004*, 14 March 2004 through 17 March 2004, pp. 138.

Juels, A. & Weis, S.A. 2006, *Authenticating pervasive devices with human protocols*, Santa Barbara, CA edn.

Juels, A. 2005, "Strengthening EPC tags against cloning", *Proceedings of the 4th ACM workshop on Wireless security*ACM, New York, NY, USA, pp. 67.

Juels, A., Rivest, R.L. & Szydlo, M. 2003, "The blocker tag: selective blocking of RFID tags for consumer privacy", *Proceedings of the 10th ACM conference on Computer and communications security*ACM, New York, NY, USA, pp. 103.

Kapoor, G. & Piramuthu, S. 2012, "Single RFID tag ownership transfer protocols", *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews,* vol. 42, no. 2, pp. 164-173.

Kapoor, G., Zhou, W. & Piramuthu, S. 2008, "Distance bounding protocol for multiple RFID tag authentication", *5th International Conference on Embedded and Ubiquitous Computing, EUC 2008*, 17 December 2008 through 20 December 2008, pp. 115.

Kara, O., Kardaş, S., Bingöl, M.A. & Avoine, G. 2010, *Optimal security limits of RFID distance bounding protocols*, Istanbul edn.

Kardaş, S., Kiraz, M.S., Bingöl, M.A. & Demirci, H. 2012, *A novel RFID distance bounding protocol based on physically unclonable functions*, Amherst, MA edn.

Karkkainen, M. 2003, "Increasing efficiency in the supply chain for short shelf life goods using RFID tagging", *International Journal of Retail & Distribution Management,* vol. 31, no. 10, pp. 529-536.

Karlins, M. & Abelson, H.I. 1970, *Persuasion, how opinion and attitudes are changed,* HarperCollins Distribution Services; Edición: 2nd Revised edition (10 de julio de 1970), ISBN-10: 0258967951.

Karlsen, K.M., Olsen, P. & Donnelly, K.A.-. 2010, "Implementing traceability: Practical challenges at a mineral water bottling plant", *British Food Journal,* vol. 112, no. 2, pp. 187-197.

Karygiannis, A.T., Eydt, B., Barber, G., Bunn, L. & Phillips, T. 2007, *Guidelines for Securing Radio Frequency Identification (RFID) Systems*, The National Institute of Standards and Technology (NIST).

Karygicmnis, A., Phillips, T. & Tsibertzopoulos, A. 2006, "RFID Security: A Taxonomy of Risk", *Communications and Networking in China, 2006. ChinaCom '06. First International Conference on*, pp. 1.

Kaur, D. & SenGupta, J. 2012, "A Trust Model Based on P2P Trust Models for Secure Global Grids", *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, pp. 1103.

Kfir, Z. & Wool, A. 2005, "Picking Virtual Pockets using Relay Attacks on Contactless Smartcard", *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*, pp. 47.

Khor, J.H., Ismail, W., Younis, M.I., Sulaiman, M.K. & Rahman, M.G. 2010, "Security Problems in an RFID System", *Wireless Personal Communications,* , pp. 1-10.

Kim, C.H. & Avoine, G. 2011, "RFID distance bounding protocol with mixed challenge", *IEEE Transactions on Wireless Communications*, Vol. 10, Nº. 5, pp. 1618 - 1626.

Kim, C.H., Avoine, G., Koeune, F., Standaert, F.-. & Pereira, O. 2009, *The Swiss-Knife RFID distance bounding protocol*, Seoul edn.

Koralalage, K.H.S.S., Reza, S.M., Miura, J., Goto, Y. & Cheng, J. 2007, "POP method: An approach to enhance the security and privacy of RFID systems used in product lifecycle with an anonymous ownership transferring mechanism", *Proceedings of the ACM Symposium on Applied Computing,* , pp. 270-275.

Kuhlen, R. 1999, *Die Konsequenzen von Informationsassistenten : Was bedeutet informationelle Autonomie oder wie kann Vertrauen in elektronische Dienste in offenen Informationsmärkten gesichert werden?* Suhrkamp Verlag, Frankfurt.

Kvarnström, B. & Vanhatalo, E. 2010, "Using RFID to improve traceability in process industry: Experiments in a distribution chain for iron ore pellets", *Journal of Manufacturing Technology Management,* vol. 21, no. 1, pp. 139-154.

Lampson, B. 1969, "DYNAMIC PROTECTION STRUCTURES", vol. 35, pp. 27-38.

Landt, J. 2005, "The history of RFID", *Potentials, IEEE,* vol. 24, no. 4, pp. 8-11.

Laurie, A. 2007, "Practical attacks against RFID", *Network Security,* vol. 2007, no. 9, pp. 4-7.

Lee, S.C. 2003, "An Introduction to Identity Management, SANS Institute.

Lee, S.M., Sang-hyun Park, Yoon, S.N. & Seung-jun Yeon 2007, "RFID based ubiquitous commerce and consumer trust", *Industrial Management & Data Systems,* vol. 107, no. 5, pp. 605-617.

Lei Zhu & Yum, T.-.P. 2011, "A critical survey and analysis of RFID anti-collision mechanisms", *Communications Magazine, IEEE,* vol. 49, no. 5, pp. 214-221.

Lenstra, A.K. & Verheul, E.R. 2001, "Selecting Cryptographic Key Sizes", *Journal of Cryptology,* vol. 14, no. 4, pp. 255-293.

Li, Z., Gong, G. & Qin, Z. 2010, *Secure and efficent LCMQ entity authentication protocol*, University of Waterloo.

Lim, C. & Kwon, T. 2006, "Strong and Robust RFID Authentication Enabling Perfect Ownership Transfer" in *Information and Communications Security*, eds. P. Ning, S. Qing & N. Li, Springer Berlin / Heidelberg, , pp. 1-20.

Linden, M. 2009, *Organisational and Cross-Organisational Identity Management*, thesis, Tampere University of Technology. Publication 779, ISBN 978-952-15-2077-8.

López, A.M., Pascual, E., Salinas, A.M., Ramos, P. & Azuara, G. 2009, "Design of a RFID based traceability system in a slaughterhause", *Workshops Proceedings of the 5th International Conference on Intelligent Environments*, eds. M. Schneider, Alexander Kröner, Julio C. Encinas Alvarado, et al, IOS Press, , pp. 67.

Lyu, J., Chang, S. & Chen, T. 2009, "Integrating RFID with quality assurance system – Framework and applications", *Expert Systems with Applications,* vol. 36, no. 8, pp. 10877-10882.

Mai, N., Sigurdur, G.B., Arason, S., Sveinn Víkingur Árnason & Thórólfur, G.M. 2010, "Benefits of traceability in fish supply chains – case studies", *British Food Journal,* vol. 112, no. 9; 0007-070, pp. 976-1002.

Maliki, T.E. & Seigneur, J. 2007, "A survey of user-centric identity management technologies", *International Conference on Emerging Security Information, Systems and Technologies,* .

Maltsbarger, R. & Kalaitzandonakes, N. 2000, "Direct and hidden costs in identity preserved supply chains", *AgBioForum,* vol. 3, no. 4, pp. 236-242.

Marimon, R., Nicolini, J.P. & Teles, P. 2000, "Competition and reputation", *Proceedings of the World Conference Econometric Society, Seattle,* .

Marsh, S. 1994, "Formalising trust as a computational concept", *University of Stirling.*

Matos, C.A.d., Trindade Ituassu, C. & Vargas Rossi, C.A. 2007, "Consumer attitudes toward counterfeits: a review and extension", *Journal of Consumer Marketing,* vol. 24, no. 1, pp. 36-47.

McFarlane, D., Sarma, S., Chirn, J.L., Wong, C.Y. & Ashton, K. 2003, "Auto ID systems and intelligent manufacturing control", *Engineering Applications of Artificial Intelligence,* vol. 16, no. 4, pp. 365-376.

Mehrjerdi, Y.Z. 2011, "RFID: The big player in the libraries of the future", *Electronic Library,* vol. 29, no. 1, pp. 36-51.

Menezes, A.J. 1994, *Elliptic Curve Public Key Cryptosystems,* Kluwer Academic Publishers, Norwell, MA, USA.

Mirowski, L.T. & Hartnett, J. 2007, "Deckard: a system to detect change of RFID tag ownership", *IJCSNS International Journal of Computer Science and Network Security,* vol. 7, no. 7, pp. 87-98.

Mitrokotsa, A., Rieback, M.R. & Tanenbaum, A.S. 2010, "Classifying RFID attacks and defenses", *Information Systems Frontiers,* vol. 12, no. 5, pp. 491-505.

Mitrokotsa, A., Rieback, M. & Tanenbaum, A. 2009, "Classifying RFID attacks and defenses", *Information Systems Frontiers,* vol. 12, pp. 1-15.

Miyata, T., Koga, Y., Madsen, P., Adachi, S.-, Tsuchiya, Y., Sakamoto, Y. & Takahashi, K. 2006, "A Survey on identity management protocols and

standards", *IEICE Transactions on Information and Systems,* vol. E89-D, no. 1, pp. 112-122.

Modinis, I. 2005, *Common Terminological Framework for Interoperable Electronic Identity Management. The 2005 Modinis IDM Study Team.*

Molnar, D., Soppera, A. & Wagner, D. 2005, "A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags", *LNCS,* vol. 3897, pp. 276-290.

Molnar, D. & Wagner, D. 2004, "Privacy and security in library RFID issues, practices, and architectures", *Proceedings of the 11th ACM Conference on Computer and Communications Security, CCS 2004*, eds. Pfitzmann B. & Liu P., , 25 October 2004 through 29 October 2004, pp. 210.

Mui, L., Mohtashemi, M. & Halberstadt, A. 2002, "A computational model of trust and reputation", *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*, pp. 2431.

Muller, G. & Vercouter, L. 2005, "Decentralized Monitoring of Agent Communications with a Reputation Model; Trusting Agents for Trusting Electronic Societies" in , eds. R. Falcone, S. Barber, J. Sabater-Mir & M. Singh, Springer Berlin / Heidelberg, , pp. 99-99.

Munilla, J. & Peinado, A. 2008, "Distance bounding protocols for RFID enhanced by using void-challenges and analysis in noisy channels", *Wireless Communications and Mobile Computing,* vol. 8, no. 9, pp. 1227-1232.

Munilla, J. & Peinado, A. 2007, "HB-MP: A further step in the HB-family of lightweight authentication protocols", *Computer Networks,* vol. 51, no. 9, pp. 2262-2267.

NSA2009, National Security Agency (USA) , 15/06/2009-last update, ***The Case for Elliptic Curve Cryptography***. Available: http://www.nsa.gov/business/programs/elliptic_curve.shtml [2012].

Okamoto, T. 1988, "Digital multisignature scheme using Bijective public-key Cryptosystems", *ACM Transactions on Computer Systems,* vol. 6, no. 4, pp. 432-441.

Onat, I. & Miri, A. 2009, "DiSEL: A distance based slot selection protocol for framed slotted aloha RFID systems", *2009 IEEE Wireless Communications and Networking Conference, WCNC 2009*, 5 April 2009 through 8 April 2009.

Ouafi, K., Overbeck, R. & Vaudenay, S. 2008, *On the security of HB# against a man-in-the-middle attack*, Melbourne, VIC edn.

Ozsu, M.T. & Valduriez, P. 1991, "Distributed database systems: Where are we now?", *Computer,* vol. 24, no. 8, pp. 68-78.

Patel, J., Teacy, W.T.L., Jennings, N.R. & Luck, M. 2005, "A probabilistic trust model for handling inaccurate reputation sources", *Third International Conference on Trust Management, iTrust 2005*, eds. Herrmann P., Issarny V. & Shiu S., , 23 May 2005 through 26 May 2005, pp. 193.

Pelissier, M., Jantunen, J., Gomez, B., Arponen, J., Masson, G., Dia, S., Varteva, J. & Gary, M. 2011, "A 112 Mb/s full duplex remotely-powered impulse-UWB RFID transceiver for wireless NV-memory applications", *IEEE Journal of Solid-State Circuits,* vol. 46, no. 4, pp. 916-927.

Peris-Lopez, P., Hernandez-Castro, J.C., Tapiador, J.M.E., Palomar, E. & Van Der Lubbe, J.C.A. 2010, "Cryptographic puzzles and distance-bounding protocols: Practical tools for RFID security", *4th Annual IEEE International Conference on RFID, RFID 2010*, 14 April 2010 through 15 April 2010, pp. 45.

Peris-Lopez, P., Orfila, A., Palomar, E. & Hernandez-Castro, J.C. 2011, "A secure distance-based RFID identification protocol with an off-line back-end database", *Personal and Ubiquitous Computing,* , pp. 1-15.

Peris-Lopez, P. 2008, "Lightweight Cryptography in Radio Frequency Identification (RFID) Systems", tesis doctoral, Universidad Carlos III de Madrid. Departamento de Informática, Octubre 2008.

Pillin, N., Joehl, N., Dehollain, C. & Declercq, M.J. 2008, "High data rate RFID tag/reader architecture using wireless voltage regulation", *2008 IEEE International Conference on RFID (Frequency Identification), IEEE RFID 2008*, pp. 141.

Pinyol, I. & Sabater-Mir, J. 2011, "Computational trust and reputation models for open multi-agent systems: a review", *Artificial Intelligence Review,* , pp. 1-25.

Pinyol, I., Sabater-Mir, J., Dellunde, P. & Paolucci, M. 2012, "Reputation-based decisions for logic-based cognitive agents", *Autonomous Agents and Multi-Agent Systems,* vol. 24, no. 1, pp. 175-216.

Platon 200, *La República,* Alhambra Editorial; Edición: Primera (1 de enero de 2000), ISBN-10: 842051621X.

Poghosyan, A., Gonzalez-Diaz, F., Bolotova, Y., Montealegre, F., Goda, H., Heboyan, V., Senesi, S., Marino, M., Mena, S.A., Ahmedov, Z., Golub, A., Levchuk, S., Mainville, D., Martinez, L., Panteleeva, O., Ponomarenko, I. & Jones, E. 2004, "Traceability and assurance protocols in the global food system", *International Food and Agribusiness Management Review,* vol. 7, no. 3, pp. 118-126.

Pouliot, S. & Sumner, D.A. 2008, "Traceability, liability, and incentives for food safety and quality", *American Journal of Agricultural Economics,* vol. 90, no. 1, pp. 15-27.

Rannenberg, K., Royer, D. & Deuker, A. 2009, "The Future of Identity in the Information Society: : Challenges and Opportunities", Springer-Verlag Berlin and Heidelberg GmbH & Co. K, ISBN-10: 3540884807.

Recordon, D. & Reed, D. 2006, "OpenID 2.0: A platform for user-centric identity management", *Proceedings of the Second ACM Workshop on Digital Identity Management, DIM 2006. Co-located with the 13th ACM Conference on Computer and Communications Security, CCS'06*, pp. 11.

Regan, K. & Cohen, R. 2005, "Indirect Reputation Assessment for Adaptive Buying Agents in Electronic Markets", *Business Agents and the Semantic Web workshop,* vol. 1.

Resende-Filho, M.A. & Buhr, B.L. 2007, "Economics of traceability for mitigation of food recalls costs",*Munich Personal RePEc Archive.*

Rieback, M. 2008, "Security and privacy of radio frecuency identification", Thesis Vrije Universiteit, ISBN/EAN: 978-90-5335-162-8.

Ripperger, T. 1998, " Ökonomik des Vertrauens: Analyse eines Organisations-prinzips", *Mohr Siebeck*, Tübingen 1998.

Roman, R. & Lopez, J. 2009, "Integrating wireless sensor networks and the internet: a security analysis", *Internet Research,* vol. 19, no. 2, pp. 246-259.

Royce, W.W. 1987, "Managing the development of large software systems: concepts and techniques", *Proceedings of the 9th international conference on Software Engineering,* IEEE Computer Society Press, Los Alamitos, CA, USA, pp. 328.

Sabater, J., Paolucci, M. & Conte, R. 2006, "Repage: REPutation and ImAGE among limited autonomous partners", *JASSS,* vol. 9, no. 2, pp. 117-134.

Sabater, J. & Sierra, C. 2005, "Review on Computational Trust and Reputation Models", *Artificial Intelligence Review,* vol. 24, no. 1, pp. 33-60.

Sabater, J. & Sierra, C. 2001, "REGRET: reputation in gregarious societies", *Proceedings of the fifth international conference on Autonomous agents*ACM, New York, NY, USA, pp. 194.

Safkhani, M., Bagheri, N., Sanadhya, S.K. & Naderi, M. 2011, "Cryptanalysis of improved Yeh 's authentication Protocol: An EPC Class-1 Generation-2 standard compliant protocol.", *IACR Cryptology ePrint Archive,* , pp. 426-426.

Sahin, E., Dallery, Y. & Gershwin, S. 2002, "Performance evaluation of a traceability system: An application to the radio frequency identification technology", *2002 IEEE International Conference on Systems, Man and Cybernetics*, eds. El Kamel A., Mellouli K. & Borne P., , 6 October 2002 through 9 October 2002, pp. 647.

Sandhu, R.S., Coyne, E.J., Feinstein, H.L. & Youman, C.E. 1996, "Computer role-based access control models", *Computer,* vol. 29, no. 2, pp. 38-47.

Sarac, A., Absi, N. & Dauzère-Pérès, S. 2010, "A literature review on the impact of RFID technologies on supply chain management", *International Journal of Production Economics,* vol. 128, no. 1, pp. 77-95.

Schiefer, G. 2008, "Tracking and tracing - a challenge for system organization and IT", *Journal of Information Technology In Agriculture,* vol. 3, no. 1, pp. 19-25.

Schillo, M., Funk, P., & Rovatsos, M. 1999, "Who can you trust: Dealing with deception", *Proceeding of Autonomous Agents '99 Workshop on "Deception, Fraud, and Trust in Agent Societies*, pp. 95.

Schillo, M., Funk, P. & Rovatsos, M. 2000, "Using trust for detecting deceitful agents in artificial societites", *Applied Artificial Intelligence, Special Issue on Trust, Deception and Fraud in Agent Societies,* Volume 14, Issue 8, September 2000, pages 825-848 .

Sen, S. & Sajja, N. 2002, "Robustness of reputation-based trust: Boolean case", *Proceedings of the 1st International Joint Conference on: Autonomous Agents adn Multiagent Systems*, eds. Castelfranchi C. & Johnson W.L., , 15 July 2002 through 19 July 2002, pp. 288.

Shamir, A. 1984, "Identity-based cryptosystems and signature schemes", Proceedings of CRYPTO 84 on Advances in cryptology, Springer-Verlag New York , pp. 47-53.

Shannon, C.E. 1948, "A Mathematical Theory of Communication", Bell System Technical Journal, 27, pp. 379–423 & 623–656.

Shears, P. 2010, "Food fraud – a current issue but an old problem", *British Food Journal,* vol. 112, no. 2, pp. 198-213.

Sierra, C. & Debenham, J. 2005a, "An information-based model for trust", *Proceedings Fourth International Conference on Autonomous Agents and Multi Agent Systems AAMAS-2005,* , pp. 497-504.

Sierra, C. & Debenham, J. 2005b, "An information-based model for trust", *4th International Conference on Autonomous Agents and Multi agent Systems, AAMAS*

05, eds. Dignum F., Dignum V., Koenig S., et al, , 25 July 2005 through 29 July 2005, pp. 629.

Smyth, S. & Phillips, P.W.B. 2002, "Product differentiation alternatives: Identity preservation, segregation, and traceability", *AgBioForum,* vol. 5, no. 2, pp. 30-42.

Song, B. & Mitchell, C.J. 2011, "Scalable RFID security protocols supporting tag ownership transfer", *Computer Communications,* vol. 34, no. 4, pp. 556-566.

Song, B. & Mitchell, C.J. 2008, "RFID authentication protocol for low-cost tags", *WiSec'08: 1st ACM Conference on Wireless Network Security*, 31 March 2008 through 2 April 2008, pp. 140.

Song, B. & Mitchell, C.J. 2011, "Scalable RFID security protocols supporting tag ownership transfer", *Computer Communications,* vol. 34, no. 4, pp. 556-566.

Sparling, D., Henson, S., Dessureault, S. & Herath, D. 2006, "Costs and benefits of traceability in the Canadian dairy-processing sector", *Journal of Food Distribution Research Distribution Research,* vol. 37, no. 1, pp. 154-160.

Stockman, H. 1948, "Communication by Means of Reflected Power", *Proceedings of the IRE*, pp. 1196.

Such, J.M., Espinosa, A., Garcia-Fornes, A. & Botti, V. 2011, "Partial identities as a foundation for trust and reputation", *Engineering Applications of Artificial Intelligence,* vol. 24, no. 7, pp. 1128-1136.

Sumar, S. & Ismail, H. 1995, "Adulteration of foods – past and present", *Nutrition & Food Science,* vol. 95, no. 4, pp. 11-15.

Sun, H.-. & Ting, W.-. 2009, "A Gen2-based RFID authentication protocol for security and privacy", *IEEE Transactions on Mobile Computing,* vol. 8, no. 8, pp. 1052-1062.

Tanenbaum, A.S. & Wetherall, D. 2010, *Computer networks,* 5th edn, Prentice Hall International.

Teacy, W.T.L., Patel, J., Jennings, N.R. & Luck, M. 2006, "TRAVOS: Trust and reputation in the context of inaccurate information sources", *Autonomous Agents and Multi-Agent Systems,* vol. 12, no. 2, pp. 183-198.

Tedeschi, P., Coïsson, J.D., Maietti, A., Cereti, E., Stagno, C., Travaglia, F., Arlorio, M. & Brandolini, V. 2011, "Chemotype and genotype combined analysis applied to tomato (Lycopersicon esculentum Mill.) analytical traceability", *Journal of Food Composition and Analysis,* vol. 24, no. 2, pp. 131-139.

Theuvsen, L. 2005, "Quality assurance in the agrofood sector: An organizationalsociological perspective", *Umwelt- Und Produktqualität im Agrarbereich (Environmental and Product Quality in Agriculture),* , pp. 173-181.

Tsudik, G. 2006, "YA-TRAP: Yet another trivial RFID authentication protocol", *4th Annual IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2006*, 13 March 2006 through 17 March 2006, pp. 640.

J. Turner. 1986, "New Directions in Communications (or Which Way to the Information Age)", *IEEE Communications Magazine*, Volume 24, no. 10, pp 8-15.

Tuyls, P. & Batina, L. 2006, "RFID-Tags for anti-counterfeiting", *Topics in Cryptology - CT-RSA 2006: The Cryptographers,* February 2005, 3960 LNCS, pp. 115-131.

Ubilava, D. & Foster, K. 2009, "Quality certification vs. product traceability: Consumer preferences for informational attributes of pork in Georgia", *Food Policy,* vol. 34, no. 3, pp. 305-310.

Véronneau, S. & Roy, J. 2009, "RFID benefits, costs, and possibilities: The economical analysis of RFID deployment in a cruise corporation global service supply chain", *International Journal of Production Economics,* vol. 122, no. 2, pp. 692-702.

Voulodimos, A.S., Patrikakis, C.Z., Sideridis, A.B., Ntafis, V.A. & Xylouri, E.M. 2010, "A complete farm management system based on animal identification using RFID technology", *Computers and Electronics in Agriculture,* vol. 70, no. 2, pp. 380-388.

Wang, F., Zhang, J., Mu, W., Fu, Z. & Zhang, X. 2009, "Consumers' perception toward quality and safety of fishery products, Beijing, China", *Food Control,* vol. 20, no. 10, pp. 918-922.

Want, R. 2006, "An introduction to RFID technology", *Pervasive Computing, IEEE,* vol. 5, no. 1, pp. 25-33.

Weis, S.A. 2003, *Security and privacy in radio-frequency identification devices*, Massachusetts Institute of Technology.

Weis, S.A. 2005, "Security parallels between people and pervasive devices", *Third IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom 2005 Workshops*, 8 March 2005 through 12 March 2005, pp. 105.

Wu, N.C., Nystrom, M.A., Lin, T.R. & Yu, H.C. 2005, "Challenges to global RFID adoption", *Technovation,* vol. 6, no. 12, pp. 1317-1323.

Wyld, D.C. 2006, "RFID 101: the next big thing for management", *Management Research News,* vol. 29, no. 4, pp. 154-173.

Xiao-dan Wu, Yun-feng Wang, Jun-bo Bai, Hai-yan Wang & Chao-Hsien Chu 2010, "RFID application challenges and risk analysis", *Industrial Engineering and Engineering Management (IE&EM), 2010 IEEE 17Th International Conference on*, pp. 1086.

Xiaojun, W. & Dong, L. 2006, "Value Added on Food Traceability: a Supply Chain Management Approach", *Service Operations and Logistics, and Informatics, 2006. SOLI '06. IEEE International Conference on*, pp. 493.

Yu, B. & Singh, M.P. 2003, "Detecting Deception in Reputation Management", *Proceedings of the Second International Joint Conference on Autonomous Agents and Multiagent Systems, AAMAS 03*, eds. Rosenschein J.S., Sandholm T., Wooldridge M. & Yakoo M., , 14 July 2003 through 18 July 2003, pp. 73.

Yu, B. & Singh, M.P. 2002a, "Distributed reputation management for electronic commerce", *Computational Intelligence,* vol. 18, no. 4, pp. 535-549.

Yu, B. & Singh, M.P. 2002b, "An evidential model of distributed reputation management", *Proceedings of the AAMAS,* , pp. 294-301.

Yuan, E. & Tong, J. 2005, "Attributed Based Access Control (ABAC) for web services", *2005 IEEE International Conference on Web Services, ICWS 2005*, 11 July 2005 through 15 July 2005, pp. 561.

Zacharia, G., Moukas, A. & Maes, P. 1999, "Collaborative reputation mechanisms in electronic marketplaces", *Proceedings of the 1999 32nd Annual Hawaii International Conference on System Sciences, HICSS-32*IEEE Comp Soc, Los Alamitos, CA, United States, 5 January 1999 through 8 January 1999, pp. 300.

Zanetti, D., Fellmann, L. & Capkun, S. 2010, "Privacy-preserving clone detection for RFID-enabled supply chains", *RFID, 2010 IEEE International Conference on*, pp. 37.

Zhang, J. 2009, *"Promoting honesty in electronic marketplaces: Combining trust modeling and incentive mechanism design*, University of Waterloo.